

A Searchable access control Scheme in the Internet of Things based on Dual-blockchain

Z. Mohammadhosseini Taheri¹ , M. Bayat^{2*} , P. Veysi³, F. MotieShirazi⁴

¹ Master's Degree, Shahed University, Tehran, Iran. mhtaheri.zahra2000@yahoo.com

² Associate Professor, Shahed University, Tehran, Iran (*Correspondence: mbayat@shahed.ac.ir)

³ Master's Degree, Shahed University, Tehran, Iran. peyman.veysi@shahed.ac.ir

⁴ Master's Degree, Shahed University, Tehran, Iran. fatemeh.motieshirazi@shahed.ac.ir

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 05 February 2026

Revised: 31 March 2026

Accepted: 09 April 2026

Available online: 21 April 2026

Keywords:

Internet of Things

Dual-Blockchain

Access Control

Searchable

Smart contract

ABSTRACT

Access control is recognized as one of the key elements in maintaining security and privacy within Internet of Things devices. By enforcing proper control mechanisms, the correct and secure use of system resources can be ensured. The IoT environment is characterized by three essential features: lightweight design, distribution, and dynamism. First, IoT devices, due to their limited computational and storage resources, are typically capable of performing only local operations such as minimal data storage. Therefore, implementing access control mechanisms on these devices imposes additional computational overhead. Second, the deployment of IoT devices is inherently distributed. Traditional access control methods are designed around a centralized trusted authority that stores all related information and makes access decisions based on it—an approach that can lead to issues such as processing delays, lack of synchronization, and the creation of single points of failure. Consequently, distributed access control solutions are required. In this study, a dynamic access control scheme is proposed. The design introduces optimizations aimed at reducing costs, simplifying complex cryptographic operations, ensuring timely revocation, enhancing access accuracy, enabling proper delegation of access across multiple domains, and preserving user confidentiality and privacy. System performance is improved through the use of a dynamic accumulator, which reduces communication rounds and accelerates access to authentication information. Additionally, two separate blockchain structures are employed concurrently—one dedicated to authentication and the other to integrity verification. The advantages of the proposed scheme include faster access to information, support for keyword-based search, dynamic access control, timely revocation of malicious entities, strong privacy preservation, reduced computational overhead, and fewer communication rounds. The only notable drawback is a slight increase in cost, which is negligible compared to the significant security benefits achieved.

Cite this article: Z.Mohammadhosseini Taheri¹, M. Bayat, P.Veysi, MotieShirazi, F. (2026). A Searchable access control Scheme in the Internet of Things based on Dual-blockchain. *Electronic and Cyber Defense*, 14(1), 69-90.

DOI: <https://dor.isc.ac/dor/20.1001.1.23224347.1405.14.1.5.7>

یک طرح کنترل دسترسی قابل جستجو در اینترنت اشیا مبتنی بر زنجیره قالب دوگانه

زهرا محمدحسینی طاهری^۱، مجید بیات^{۲*}، پیمان ویسی^۳، فاطمه مطیع شیرازی^۴

^۱ کارشناسی ارشد، دانشگاه شاهد، تهران، ایران. mhtaheri.zahra2000@yahoo.com

^۲ دانشیار، دانشگاه شاهد، تهران، ایران (نویسنده مسئول: mbayat@shahed.ac.ir)

^۳ کارشناسی ارشد، دانشگاه شاهد، تهران، ایران. peyman.veysi@shahed.ac.ir

^۴ کارشناسی ارشد، دانشگاه شاهد، تهران، ایران. fatemeh.motieshirazi@shahed.ac.ir

چکیده	مشخصات مقاله
کنترل دسترسی به عنوان یکی از عناصر کلیدی در حفظ امنیت و حریم خصوصی دستگاه‌های اینترنت اشیا شناخته می‌شود. با اعمال کنترل مناسب، امکان استفاده صحیح و ایمن از منابع سیستم فراهم می‌گردد. محیط اینترنت اشیا دارای سه ویژگی اساسی سبک‌وزنی، توزیع‌شدگی و پویایی است. نخست آن که دستگاه‌های اینترنت اشیا به دلیل محدودیت منابع محاسباتی و ذخیره‌سازی، عمدتاً تنها قادر به انجام عملیات محلی نظیر ذخیره‌سازی محدود داده‌ها هستند و بنابراین پیاده‌سازی مکانیزم‌های کنترل دسترسی در آن‌ها با بار محاسباتی مضاعف همراه خواهد بود. دوم آن که، استقرار این دستگاه‌ها به صورت توزیع‌شده است. روش‌های سنتی کنترل دسترسی مبتنی بر نهاد مرکزی مورد اعتماد طراحی شده‌اند که تمام اطلاعات مرتبط را ذخیره کرده و بر اساس آن تصمیم‌گیری می‌کنند؛ امری که منجر به بروز مشکلاتی از قبیل تأخیر در پردازش، عدم هم‌زمانی و ایجاد نقطه شکست می‌گردد. از این رو، استفاده از راهکارهای توزیع‌شده برای کنترل دسترسی ضروری به نظر می‌رسد. در این پژوهش، طرحی برای کنترل دسترسی پویا معرفی شده است. در این طرح، بهینه‌سازی‌هایی با هدف کاهش هزینه، ساده‌سازی محاسبات پیچیده رمزنگاری و رمزگشایی، اجرای به موقع فرایند ابطال، افزایش دقت در کنترل دسترسی، تفویض صحیح دسترسی بین دامنه‌های مختلف، حفظ محرمانگی و حریم خصوصی کاربران انجام گرفته است. بهبود عملکرد سیستم از طریق استفاده از انباشتگر پویا میسر شده است که باعث کاهش دوره‌های ارتباطی و افزایش سرعت در دسترسی به اطلاعات مربوط به احراز اصالت شده است. همچنین، به صورت هم‌زمان از دو زنجیره قالب بهره گرفته شده که به طور مجزا احراز اصالت و بررسی یکپارچگی را انجام می‌دهند. مزایای حاصل از این طرح شامل افزایش سرعت در دسترسی به اطلاعات، پشتیبانی از جستجوی مبتنی بر کلمه کلیدی، کنترل دسترسی پویا، ابطال به موقع موجودیت‌های مخرب، حفظ حریم خصوصی در سطح بالا، کاهش بار محاسباتی و کاهش تعداد دوره‌های ارتباطی می‌باشد. تنها ایراد قابل ذکر، افزایش جزئی در هزینه‌ها است که در مقایسه با مزایای امنیتی به دست آمده، قابل اغماض تلقی می‌گردد.	تاریخچه مقاله: نوع مقاله: علمی پژوهشی دریافت: ۱۴۰۴/۱۱/۱۶ بازنگری: ۱۴۰۵/۰۱/۱۱ پذیرش: ۱۴۰۵/۰۱/۲۰ ارائه آنلاین: ۱۴۰۵/۰۲/۰۱ کلید واژه‌ها: اینترنت اشیا زنجیره قالب دوگانه کنترل دسترسی قابلیت جستجو قرارداد هوشمند

استناد: زهرا محمدحسینی طاهری، مجید بیات، پیمان ویسی، مطیع شیرازی حسینی، فاطمه. (۱۴۰۵). یک طرح کنترل دسترسی قابل جستجو در اینترنت اشیا مبتنی بر زنجیره قالب دوگانه. پدافند الکترونیک و سایبری، ۱۴(۱)، ۹۰-۶۹. DOR: <https://dor.isc.ac/dor/20.1001.1.23224347.1405.14.1.5.7>

© نویسندگان حق نشر و حقوق کامل انتشار را برای خود محفوظ می‌دارند.

ناشر: دانشگاه جامع امام حسین(ع)

۱. مقدمه

قراردادهای هوشمند عدالت در دسترسی، جستجو داده‌های ذخیره شده و بررسی یکپارچگی و صحت اطلاعات فراهم می‌شود.

بنابراین، به دلیل رشد اینترنت اشیا و تولید انبوه داده‌ها توسط حسگرها و دستگاه‌ها نیاز است که این داده‌ها جمع‌آوری، به صورت ایمن ذخیره و به اشتراک گذاشته شوند. پس از فناوری زنجیره قالب برای کنترل دسترسی دقیق‌تر کمک گرفته می‌شود. همچنین نیاز به نهاد متمرکز برای احراز اصالت و راه‌اندازی سیستم از بین می‌رود.

ساختار مابقی مقاله به این شرح است که در بخش ۲ روش تحقیق و پیشینه کارهای صورت گرفته توسط نویسندگان مختلف بررسی می‌شود. سپس در بخش ۳ طرح پیشنهادی معرفی شده که به چهار زیربخش تقسیم می‌گردد: ابتدا معماری طرح پیشنهادی معرفی می‌شود. سپس در ادامه به بررسی نحوه اجرای طرح پرداخته می‌شود و در ادامه ویژگی‌های طرح پیشنهادی ذکر خواهد شد. در نهایت طرح پیشنهادی با طرح‌های گذشته مشابه مقایسه می‌گردد. در بخش ۴ الگوریتم اجماع PBFT با استفاده از ویژوال استودیو و زبان پایتون پیاده‌سازی شده و تأخیر اجماع بر اساس افزایش تعداد گره‌ها بررسی می‌شود. در نهایت در بخش ۵ نتیجه‌گیری ارائه می‌شود.

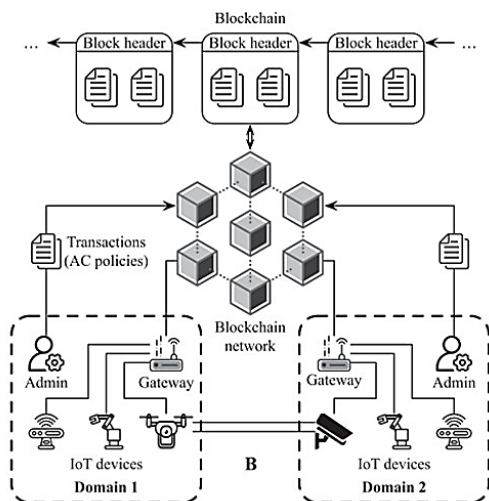
جدول (۱). نمادها

نماد	توضیحات
U_i	کاربران
D_i	دستگاه‌ها
GW_i	دروازه
En_i	گره لبه
LDA	مرجع دامنه محلی
GDA	مرجع دامنه جهانی
BC_i	زنجیره قالب
CN	گره ابری
PP	پارامتر عمومی سیستم
λ	پارامتر امنیتی راه‌اندازی سیستم
Atr	ویژگی‌ها

اینترنت اشیا کاربرد بسیاری در زندگی بشر دارد. برای مثال، دستگاه‌های اینترنت اشیا در شهرهای هوشمند، تأسیسات، خانه‌ها، مراکز نظامی و محیط‌های تهاجمی مستقر شده‌اند. چنین دستگاه‌هایی می‌توانند ردیابی کاربران و محیط را آسان کرده و داده‌های خصوصی را جمع‌آوری کنند. شرکت بین‌المللی داده تخمین می‌زند که مقدار داده‌های تولید شده توسط دستگاه‌های اینترنت اشیا ممکن است در سال ۲۰۲۵ به $4/79^{1}$ ZB برسد [۱]. زنجیره قالب به عنوان یک راه‌حل برای مدیریت توزیع شده و پاسخگویی در شبکه‌های اینترنت اشیا مطرح شده است. امنیت اینترنت اشیا توسط زنجیره قالب افزایش داده می‌شود، زیرا هر گره برای تأیید تراکنش‌های جدید در سراسر شبکه درگیر می‌شود [۲]. اما پیاده‌سازی فناوری زنجیره قالب به طور مستقیم در شبکه‌های اینترنت اشیا نیازمند هزینه‌های بالا و انرژی زیادی است [۳]؛ بنابراین از فناوری محاسبات لبه، ابر، مه برای جلوگیری از این مشکلات استفاده می‌شود. همچنین، برای مهار حمله‌های امنیتی رایج در اینترنت اشیا، باید مکانیسم‌های امنیتی ضروری ایجاد شوند [۴]. یک شبکه اینترنت اشیا باید شامل حریم خصوصی، احراز اصالت، تأیید، کنترل دسترسی، حفاظت از داده‌ها و مدیریت اعتماد باشد [۳]. کنترل دسترسی یک مکانیسم امنیتی است که دسترسی قانونی و کنترل شده به منابع حیاتی و محدود در اینترنت اشیا را تضمین می‌کند [۴]. در اینترنت اشیا دستگاه‌ها، حسگرها و اشیا فیزیکی توزیع شده هستند و هم‌زمان حجم عظیمی از داده‌ها را تولید می‌کنند. دستگاه‌ها در دامنه‌های مختلفی مستقر شده که برای ارتباط بین دامنه‌ای و تبادل اطلاعات نیاز به احراز اصالت متقابل دامنه‌ای است. برای کاهش بار محاسبات از سرورهای لبه و ابری کمک گرفته می‌شود تا سمت کاربران بار محاسباتی کاهش یابد. از فناوری زنجیره قالب برای برقراری امنیت، یکپارچگی، قابلیت ردیابی تراکنش‌ها، تغییرناپذیری^۲ استفاده می‌شود. داده‌های تولید شده باید به طور ایمن و محرمانه ذخیره شوند، به اشتراک گذاشته شوند و امکان کنترل دسترسی بر روی آن‌ها وجود داشته باشد؛ بنابراین از طرح رمزگذاری مبتنی بر ویژگی می‌توان استفاده کرد که محرمانگی، اصالت داده‌ها، کنترل دسترسی را فراهم می‌کند و مالک داده با تعریف کردن سیاست دسترسی، ویژگی‌های لازم برای بازیابی و اشتراک‌گذاری داده‌های خود را فراهم می‌کند و با استفاده از زنجیره قالب تمام اطلاعات ثبت می‌شوند و قابل ردیابی خواهند بود. برای کنترل دسترسی بر روی داده‌ها می‌توان از قابلیت جستجو مبتنی بر کلمه کلیدی که توسط مالک داده ایجاد شده، استفاده کرد تا بازیابی سریع‌تر انجام شود. همچنین با استفاده از

^۱. Zeta Byte.^۲. Immutability.

در این دامنه‌ها توسط مدیر دامنه و سرور دامنه و مکانیزم RBAC انجام می‌شود و مدیر دامنه مسئول احراز اصالت دستگاه‌های دامنه است و مطابق شکل ۱ معماری ساختار ۵ لایه دارد.



شکل (۱). شماتیک طرح cross-domain [۱]

این سیستم از سه بخش تشکیل شده است: زنجیره قالب، شبکه زنجیره قالب، پایانه‌های اینترنت اشیا و گره‌های خدمات و دامنه کنترل دسترسی.

زنجیره قالب: زنجیره قالب در مدل سیستم پیشنهادی، تراکنش‌ها و قراردادهای هوشمند قابل اجرا را ذخیره می‌کند. با استفاده از الگوریتم‌های رمزنگاری و الگوریتم‌های اجماع، تراکنش‌ها و قراردادهای هوشمند نمی‌توانند بدون شناسایی دست‌کاری شوند. تمامی سوابق عملیاتی و وضعیت قراردادهای هوشمند قابل‌ردیابی و ممیزی هستند.

شبکه زنجیره قالب: سیاست‌های کنترل دسترسی در شبکه زنجیره برای تثبیت سرویس کنترل دسترسی در حال استقرار و اجرا هستند.

دامنه کنترل دسترسی: در سیستم پیشنهادی، تمام پایانه‌های اینترنت اشیا و سایر دستگاه‌های شبکه را به دامنه‌های کنترل دسترسی مختلف تقسیم کردند. طراحی دامنه کنترل دسترسی، مانع از دسترسی دستگاه‌های دامنه‌های مختلف به یکدیگر نمی‌شود. از طریق تنظیمات مدیریت، این دستگاه‌ها می‌توانند به‌صورت قانونی و تحت حفاظت به یکدیگر دسترسی داشته باشند. از مدل RBAC بین دامنه‌ای برای دستیابی به کنترل دسترسی بین دستگاه‌ها از دامنه یکسان یا متفاوت استفاده می‌شود.

گره‌های خدمات زیادی در طرح پیشنهادی برای حفظ برخی از عملیات سیستم و ارائه خدمات برای پایانه‌های اینترنت اشیا وجود دارد. گره‌های سرویس، گره‌هایی مانند (ذخیره‌سازی متصل به شبکه^۲) و سرورهای (رابط برنامه‌نویسی کاربردی^۳) هستند که

W	مجموعه ویژگی
W	کلمه کلیدی
OU	مالک داده
U	کاربر
D	دستگاه
SK	کلید مخفی
OSK	کلید برون‌سپاری
USK	کلید مخفی کاربر
MSK	کلید مخفی اصلی
Knd	داده
CT	متن رمزی
Req	درخواست
Td	دریچه
TK	کلید تبدیل
SC	قرارداد هوشمند
TCT	متن رمزی تبدیل شده
(M,P)	ساختار دسترسی
V	عدد اول مقسوم علیه
S	عدد تصادفی
U	کلید مخفی رمزگشایی

۲. روش تحقیق

شیانوهان‌ها^۱ و همکاران مفهوم دامنه‌های متقاطع را در مقاله [۱] مطرح کردند. یعنی دستگاه‌ها در دامنه‌های مختلف تقسیم‌بندی می‌شوند و برای دسترسی به هر دامنه باید طرح کنترل دسترسی و تفویض دسترسی تعریف شود. برای دسترسی بین دامنه‌ای از مکانیزم کنترل دسترسی RBAC استفاده می‌شود. تفویض دسترسی

^۲. Network attached storage.

^۳. Application Programming Interface.

^۱. Xiaohan Ha.

در لایه داده، انواع تراکنش‌های جدید، مانند تراکنش مدیر، تراکنش کاربر و تراکنش پایه دسترسی، برای دستیابی به یک سیستم کنترل دسترسی خودکار طراحی شده‌اند. علاوه بر این، سیستم از خروجی تراکنش‌های قابل استفاده مجدد^۱ و خروجی تراکنش‌های مصرف نشده^۲، برای ردیابی سوابق عملیات هر موجودیت به راحتی استفاده می‌کند. در لایه شبکه پروتکل‌های شبکه اینترنت اشیا موجود و سازوکارهای انتقال مانند MQTT و Coap کاربردی که سازگار با سیستم پیشنهادی هستند و مستقیماً از این طرح‌ها استفاده می‌شود. در لایه اجماع، از پروتکل توافقی PBFT استفاده می‌شود. در لایه قرارداد، کدهای عملیاتی برای اجرای عملیات مختلف مورد نیاز نهادها طراحی می‌شوند. در لایه برنامه، یک سیستم کنترل دسترسی مبتنی بر نقش متقابل مستقل توزیع شده شامل مدیریت کنترل دسترسی، مجوز دسترسی، ممیزی و کیف پول پیشنهاد می‌شود.

از بین تمامی مقالات مطالعه شده برای بررسی یک طرح کنترل دسترسی در اینترنت اشیا مبتنی بر زنجیره قالب به عنوان مقاله پایه از [۲] استفاده شده است. این طرح توسط سوهیر^۳ و همکاران مطرح شده است.

در این طرح دامنه‌های مختلفی وجود دارد. در دامنه‌ها کاربران و دستگاه‌ها قرار می‌گیرند و هر دامنه شامل یک مرجع دامنه محلی یا دامنه محلی است که ویژگی‌های کاربران و دستگاه‌ها را دریافت کرده و برای آن‌ها کلید ایجاد می‌کند. همچنین ویژگی‌ها در LL^۴ هر دامنه ذخیره می‌شود.

در هر دامنه به طور جداگانه اجزایی وجود دارد:

Devise	User
LDA ^۶	LL
EN	GW ^۵

در هر دامنه یک دروازه وجود دارد که مبتنی بر احراز اصالت فیلتر درخواست را برای کاهش سربار و حملات انکار سرویس انجام می‌دهد و فقط کاربران مجاز درخواستشان ثبت و بررسی می‌شود. سپس دروازه درخواست فیلتر شده را برای گره‌های لبه ارسال می‌کند و گره لبه وظیفه تفویض دسترسی را انجام می‌دهد و با الگوریتم بهینه‌سازی RHSO گره‌های نماینده برای تفویض دسترسی انتخاب می‌شود. اگر درخواست برای خود دامنه و مجاز باشد، درخواست انجام می‌شود؛ اما اگر درخواست برای خارج دامنه باشد لبه ویژگی درخواست‌کننده همراه با درخواست را از طریق یک کانال مخفی برای لبه دامنه هدف

می‌توانند منابع دسترسی یا دسترسی به دستگاه‌های بسیاری را به دست آورند. آن‌ها منابع محاسباتی و منابع ذخیره‌سازی کافی برای دسترسی مستقیم به شبکه زنجیره قالب را دارند.

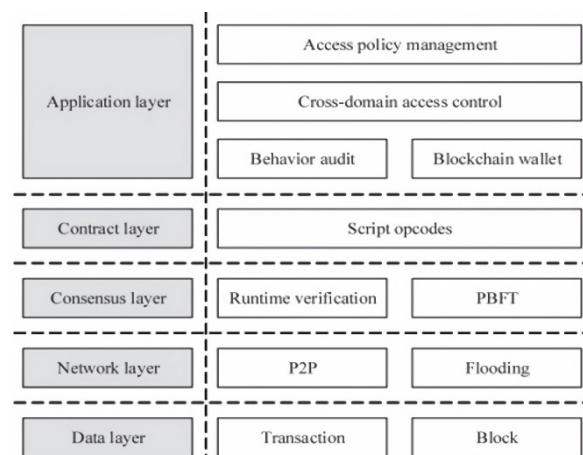
گره‌های کامل: گره کامل مسئول حفظ شبکه زنجیره قالب و دفترکل زنجیره، دریافت و پردازش تراکنش‌ها از مدیران و پایانه‌های اینترنت اشیا و بسته‌بندی تراکنش‌های قانونی در بلوک‌ها و همگام‌سازی این بلوک‌ها از طریق یک پروتکل اجماع هستند.

مدیر: مجوزهای کنترل دسترسی همه دستگاه‌ها را در دامنه کنترل دسترسی مدیریت می‌کند، نقش‌هایی را برای دستگاه‌ها تنظیم می‌کند و منابعی را که نقش‌ها می‌توانند به آن‌ها دسترسی داشته باشند را پیکربندی می‌کند. برای دستیابی به کنترل دسترسی متقابل دامنه، مدیر همچنین نیاز به مدیریت پینگ نقشه بین نقش‌های سایر دامنه‌ها و نقش‌های دامنه خود دارد.

دروازه‌ها: باتوجه به محدودیت منابع محاسباتی، تکمیل تمام عملکردهای زنجیره قالب برای دستگاه‌های اینترنت اشیا چالش برانگیز است. دروازه‌ها گره‌های کاملی از زنجیره هستند که می‌توانند برای کمک به پایانه‌های دیگر برای تأیید مجوز دسترسی استفاده شوند.

پایانه‌های دیگر: پایانه‌های دیگری نیز وجود دارند که می‌توان در دامنه کنترل دسترسی به آن‌ها دسترسی داشت، مانند سرویس ذخیره‌سازی، برخلاف دستگاه‌های اینترنت اشیا، این پایانه‌ها می‌توانند به عنوان گره‌های یک دامنه عمل کنند. این پایانه‌ها اشیا اصلی هستند که توسط شبکه زنجیره قالب ارائه می‌شوند و داده‌های شبکه‌های زنجیره را ذخیره می‌کنند.

سیستم پیشنهادی مبتنی بر طراحی معماری زنجیره قالب پنج لایه است که شامل لایه‌های داده، شبکه، اجماع و کاربرد است. ساختار ترکیب سیستم پیشنهادی در شکل ۲ نشان داده شده است.



شکل (۲). نمای طرح [۱]

^۱. Reusable transaction (RTXO).

^۲. Unspent transaction (UTXO).

^۳. Suhair.

^۴. Local ledger.

^۵. Gate Way.

^۶. Local Domain Authority.

کلیدی انجام می‌شود. همچنین با بهره‌گیری از قراردادهای هوشمند عدالت و انصاف در طرح رعایت می‌گردد و رمزنگاری و رمزگشایی دوزخه‌ای در طرح به کار گرفته می‌شود. کلمه کلیدی مرتبط توسط مالک ایجاد و رمز می‌گردد.

برای یک شبکه هوشمند مبتنی بر زنجیره قالب و گره‌های مه چن^۳ و همکاران طرح ارائه شده در [۴] را معرفی کردند. در این مقاله از دوزخه قالب به طور هم‌زمان استفاده شده است. یکی از زنجیره‌ها به جای یک سیستم PKI سنتی به کار گرفته شده و برای احراز اصالت مورد استفاده قرار گرفته است و زنجیره دیگر برای ممیزی و بررسی یکپارچگی به کاررفته و چکیده‌های متون رمزی در آن ذخیره شده‌اند. در این طرح یک شبکه هوشمند به همراه گره‌های مه که از منابع محاسباتی کافی برخوردارند، در نظر گرفته شده است. در این طرح گره‌های مه احراز اصالت می‌شوند و اطلاعات هویتی آن‌ها با امضا قابل‌بررسی و تصدیق است و این اطلاعات در زنجیره قالب اول ذخیره می‌گردد. همچنین یک سرور ابری در نظر گرفته شده که متن رمزی توسط گره‌های مه در آن ذخیره می‌شود و چکیده آن در زنجیره ثبت می‌گردد. پس از آن که گره‌های مه احراز اصالت شده‌اند، به طور انبوه داده‌ها را از شبکه جمع‌آوری کرده و سپس برای انتقال داده‌ها به سرور ابری با پروتکل توافق کلید تأیید شده با ابر ارتباط گرفته و انتقال داده‌ها انجام می‌پذیرد. همچنین در این طرح از رمزگذاری برخط و برون‌خط پشتیبانی شده و زمانی که منابع محاسباتی کافی وجود دارد، بعضی از پیش محاسبات برون‌خط انجام می‌شوند. همچنین از طرح تجمعی بدون گواهی برای کاهش مدیریت گواهی‌های پیچیده استفاده شده است.

از گره‌های مه احراز اصالت شده به‌عنوان پردازنده‌های محلی استفاده می‌شود. KGC سرور قابل‌اعتماد است که مسئول راه‌اندازی سیستم و تولید کلید در نظر گرفته شده و برای مدیریت کلیدها با زنجیره قالب همکاری می‌کند. SMها دستگاه‌های پایانی اینترنت اشیا هستند که به مدل‌های امنیتی برای ذخیره کلیدهای مخفی و نام مستعار مجهز شده‌اند. فضای ذخیره‌سازی ابری^۴ یک سرور مرکزی برای ذخیره اطلاعات تاریخچه شبکه هوشمند است. مرکز کنترل^۵ به داده‌ها از فضای ذخیره‌سازی ابری دسترسی داشته، درحالی‌که فضای ذخیره‌سازی ابری ممکن است در معرض خطر قرار گیرد (به طور کامل قابل‌اعتماد نباشد). مرکز کنترل مجموعه‌ای از سرورهای غنی از منابع است. زنجیره قالب دو دفترکل توزیع شده دارای مجوز مستقل به نام‌های زنجیره کاربر و زنجیره داده، تعریف شده است. همچنین یک طرح FB-ASC برای کاهش قرارداد هوشمند سنگین معرفی شده است.

ارسال و تفویض دسترسی انجام می‌شود. یک ساختار سلسله‌مراتبی به علت وجود مرجع دامنه محلی و مرجع دامنه جهانی^۱ GDA که در سرور ابری قرار دارد، به وجود می‌آید.

مرجع دامنه محلی بر اساس الگوریتم منحنی فرا بیضوی کلید و احراز اصالت را انجام می‌دهد که از نظر اندازه پیام نسبت به منحنی بیضوی بهینه‌تر است، همچنین یک سرور ابری وجود دارد که داده‌ها در آنجا ذخیره می‌شوند و برای اشتراک‌گذاری داده‌ها و اطمینان از حریم خصوصی، بیش از بارگذاری در ابر با حریم خصوصی دیفرانسیل رمز می‌شود. نوپزی که به‌وسیله لاپلاس ایجاد و با کد اصلی رمز می‌شود و بعد در ابر بارگذاری می‌گردد.

همچنین در این طرح ابطال دوگانه ویژگی‌های کاربر و کاربر تعریف شده است که منجر به کنترل دسترسی پویا می‌شود. ویژگی کاربر با زمان انقضا باطل و کاربر بر اثر رفتار مخرب باطل می‌شود و کاربری که باطل شده نمی‌تواند داده‌ای در ابر بارگذاری و یا درخواست کند. برای این کار باید درخواست مجدد تولید کلید به مرجع دامنه محلی ارسال کند.

یک طرح جستجوی کلمه کلیدی مبتنی بر رمزنگاری^۳ [توسط هوانگ^۲ و همکاران ارائه شده است. این طرح برای یک سیستم مراقبت بهداشتی و اشتراک پرونده‌های بهداشتی طراحی شده، تعدادی مالک داده وجود دارد که مقصود همان بیماران است. هر بیمار پرونده بهداشتی مربوط به خویش را رمز و در سرور ابری قرار می‌دهد و از رمزنگاری ABSE استفاده می‌شود و سپس همان مالک داده کلمه کلیدی مرتبط با داده خودش را ایجاد و رمز جزئی صورت می‌گیرد و در سرور لبه بارگذاری می‌کند تا رمزنگاری آن تکمیل شود. هرگاه کاربری مثل یک پزشک درخواست دسترسی به داده‌ای داشته باشد، این درخواست به زنجیره قالب ارسال می‌شود و زنجیره با جستجو و اجماع هویت را شناسایی و درخواست برای سرور ابری ارسال می‌شود و سرور ابری بر اساس کلمه کلیدی که دریافت کرده پرونده رمز شده مربوطه را برای سرور لبه ارسال و توسط سرور لبه رمزگشایی جزئی انجام می‌شود. ولی سرور قادر به بازیابی کلید خصوصی نخواهد بود و سپس پرونده در اختیار پزشک قرار خواهد گرفت و رمزگشایی آن تکمیل می‌گردد. این طرح کاربر دوستانه است؛ چون کاربران فقط رمزنگاری و رمزگشایی جزئی انجام می‌دهند و قابلیت جستجوی کلمه کلیدی وجود دارد. چون ABSE از نظر محاسباتی بار سنگینی را ایجاد خواهد کرد از سرور ابری و لبه کمک گرفته می‌شود. در این سیستم یک مرجع قابل‌اعتماد وجود دارد که طرفین برای احراز اصالت و دریافت کلید معتبر باید با آن ارتباط برقرار کنند. در این مقاله کنترل دسترسی بر اساس ویژگی و جستجوی کلمه

^۳. Liquan Chen.

^۴. Cloud Storage Server.

^۵. Control center.

^۱. Global Domain Authority.

^۲ Hancheng Gao

ضروری در صورت رفتار مخرب، ناشناس ماندن در دسترسی به اطلاعات و حفظ حریم خصوصی پرداخته می‌شود. برای رفع مشکلات و چالش‌های مقیاس‌پذیری و توزیع‌شدگی اینترنت اشیا از زنجیره‌های قالب استفاده می‌گردد. برای کاهش سربار محاسباتی و دوره‌های ارتباطی از مراکز احراز اصالت، سرورهای ابری و لبه استفاده شده و برای کنترل دسترسی به موقع فیلترکردن درخواست‌ها انجام می‌پذیرد. در طرح پیشنهادی قراردادهای هوشمند افزوده خواهد شد تا عدالت و انصاف در دسترسی بر مبنای مقاله [۳] جستجو و ابطال به موقع بر مبنای [۵] انجام می‌پذیرد. همچنین برای کاهش دور ارتباطی و سربار محاسباتی احراز اصالت از انباشتگرهای پویا^۲ در مقاله [۶] استفاده خواهد شد، تا تأخیر اجماع زنجیره قالب با افزایش تعداد تراکنش‌ها کاهش یافته و طرح [۲] بهینه گردد. به طرح پایه [۲] مؤلفه‌هایی نظیر قرارداد هوشمند، رمزگشایی جزئی، جستجو مبتنی بر کلمه کلیدی و دریچه و رمزنگاری مبتنی بر ویژگی افزوده شده تا کنترل دسترسی به شکل بهینه‌تری ارائه گردد.

۳. طرح پیشنهادی

در بررسی مقالات مختلف در حوزه اینترنت اشیا درک شد که کنترل دسترسی سنتی وابسته به یک نهاد متمرکز، با حملات مختلفی مواجه خواهد شد. برای حل این چالش از زنجیره قالب استفاده شده است. در طرح پیشنهادی قابلیت ثبت نام کاربران و احراز اصالت سریع‌تر فراهم شده و بررسی احراز اصالت با کمک انباشتگر پویا برای کاهش تأخیر انجام می‌شود. در این طرح از سرورهای لبه برای تفویض دسترسی بین دامنه‌ها استفاده شده تا بار محاسباتی کاهش یابد. کنترل دسترسی پویا با ابطال به موقع کاربران و ویژگی‌های آن‌ها فراهم شده است. همچنین از گره‌های دروازه برای فیلترکردن درخواست‌ها استفاده شده تا پاسخ‌ها از نظر زمانی سریع‌تر دریافت شوند. سرورهای ابری برای اشتراک‌گذاری و ذخیره‌سازی داده‌ها در طرح گنجانده شده‌اند و داده‌ها با رمزنگاری توسط کاربر در ابر ذخیره می‌گردد. برای توزیع‌شدگی و مقیاس‌پذیری به صورت هم‌زمان از دوزنجیره قالب جدا برای احراز اصالت و بررسی یکپارچگی استفاده شده و همچنین برای مدیریت بهتر از رمزگشایی جزئی، برون‌سپاری و قرارداد هوشمند بهره گرفته شده است.

۳-۱. معماری طرح پیشنهادی

اینترنت اشیا به صورت دامنه‌های مختلف فرض می‌گردد. در هر دامنه دستگاه و کاربرانی وجود دارد که داده‌هایی را تولید و به اشتراک گذاشته و باید این داده‌ها به صورت ایمن ذخیره شوند. از سرورهای ابری برای ذخیره‌سازی امن داده‌ها استفاده شده است. در شکل ۳ مدل کلی معماری نمایش داده شده است.

با توسعه سریع اینترنت اشیا، توسط میلیون‌ها دستگاه دائماً حجم عظیمی از داده‌ها تولید می‌گردد. توسعه هوش مصنوعی و محاسبات لبه امکان انجام تجزیه و تحلیل داده‌ها و استخراج دانش را به طور کارآمد در میان دستگاه‌های لبه اینترنت اشیا فراهم آورده است. دانش، ازجمله نتایج میانی و مدل‌های آموزشی به دست آمده از مقادیر زیادی داده‌ی اضافی، هسته و پایه هوش لبه‌ها تلقی می‌شود. بالاین حال، اشتراک و استفاده از دانش همچنان با یک سری مسائل امنیتی و حریم خصوصی مانند دسترسی غیرقانونی به دانش، دست‌کاری لبه دانش و نشت حریم خصوصی مواجه شده است. برای پرداختن به این مسائل، در مقاله [۵]، جینگ وانگ^۱ و همکاران یک معماری مبتنی بر زنجیره قالب و ذخیره دانش را پیشنهاد کرده‌اند که مدیریت دانش ایمن را در اینترنت اشیا هوشمند ممکن می‌سازد. ابتدا یک طرح ذخیره دانش غیرمتمرکز و قابل اعتماد مبتنی بر زنجیره طراحی می‌گردد که شامل ذخیره‌سازی دانش رمزگذاری شده روی زنجیره و یک پروتکل همسو با اثبات واگذار شده^۲ بهبودیافته است. علاوه بر این، یک مکانیسم اشتراک‌گذاری دانش رمزگذاری شده قابل جستجو مبتنی بر ویژگی‌های سبک‌وزن پیشنهاد شده است که در آن همکاری دانش دقیق و حفظ حریم خصوصی از طریق قراردادهای هوشمند و جستجوی کلمات کلیدی حاصل خواهد شد. علاوه بر این، سربار محاسباتی دستگاه‌های لبه از طریق طراحی رمزگشایی جزئی برون‌سپاری کاهش داده می‌شود.

(۱) معماری ذخیره‌سازی و اشتراک‌گذاری دانش سبک‌وزن مبتنی بر زنجیره قالب با مجوز یکپارچه پیشنهاد شده که استفاده از دانش و همکاری ایمن را در اطلاعات زیادی ممکن ساخته است.

(۲) گواهی تفویض شده بهبودیافته مبتنی بر شهرت طراحی می‌گردد. پروتکل اجماع سهام برای دستیابی به اعتماد و سازگاری چندجانبه بین گره‌های ذخیره‌سازی در طرح استفاده شده است.

(۳) یک طرح به اشتراک‌گذاری دانش قابل جستجوی ریز پیشنهاد شده که به کاربران اجازه داده تا از طریق تنظیم کلمات کلیدی مشخصه با خط‌مشی‌های دسترسی مختلف، دانشی از علایق خود به دست آورند. امنیت و حریم خصوصی دانش از طریق بازیابی متن رمزی ذخیره شده با قراردادهای هوشمند تضمین شده است.

(۴) معماری سبک‌وزن بودن را ممکن کرده و بخشی از محاسبه رمزگشایی به سرور لبه بارگذاری می‌گردد و کارایی محاسباتی دستگاه‌های اینترنت اشیا بهبود یافته است.

در طرح پیشنهادی، یک طرح کنترل دسترسی قابل جستجو بر مبنای مقاله [۲] ارائه می‌گردد. همچنین برای اشتراک‌گذاری و تبادل امن اطلاعات، در طرح پیشنهادی، الزامات امنیتی لازم فراهم شده و به لغو به موقع کاربران، به روزرسانی اطلاعات، ابطال

^۳. Dynamic accumulator.

^۱. Wang.

^۲. DPoS.

اطلاعات و ویژگی‌های خود (نام، ساختار دسترسی، ویژگی‌های خود) و برای دستگاه‌ها (شناسه دستگاه، نام مستعار، ویژگی، اطلاعات دستگاه، مالک، حالت دستگاه، مدت زمان اعتبار) را به مرجع ارسال کرده و بر اساس اطلاعات دریافتی احراز اصالت صورت می‌گیرد. کلید عمومی و خصوصی ایجاد شده و این اطلاعات در زنجیره قالب اول برای بررسی احراز اصالت ذخیره گشته و به کاربران ارسال می‌گردد.

۷) انباشتگر پویا: مرجع دامنه محلی اطلاعات احراز هویتی را در انباشتگر به صورت تجمع شده ذخیره کرده که در دوره‌های ارتباطی بعدی احراز اصالت سریع تر انجام شود و نیازی به مراجعه به زنجیره نخواهد بود.

۸) فضای ذخیره‌سازی ابری^۷: برای اشتراک‌گذاری امن داده‌ها، مالکان داده با استفاده از رمزنگاری مبتنی بر ویژگی داده‌ها را در فضای ابری بارگذاری خواهند کرد.

۹) مرجع دامنه جهانی^۸: در سرور ابری یک مرجع جهانی قرار داده شده که تمام اطلاعات را از مرجع دامنه محلی ذخیره کرده و نگهداری خواهد کرد.

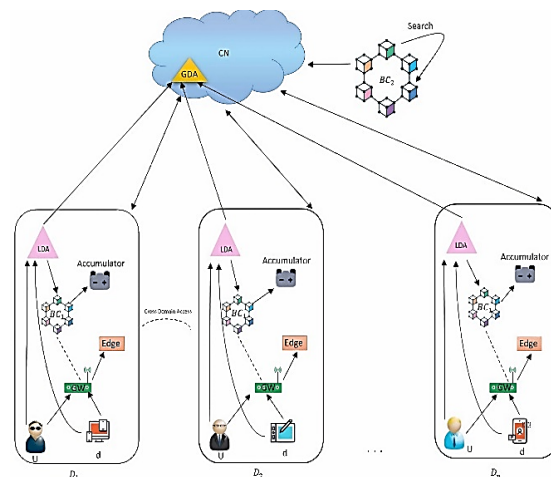
۱۰) زنجیره قالب: زنجیره قالب دوم برای بررسی هم‌زمان یکپارچگی استفاده شده و چکیده اطلاعات و تبادلات در آن ذخیره می‌گردد.

۳-۲. شرح اجرای الگوریتم طرح

گردش کار سیستم به شرح زیر است:

۱- ثبت‌نام کاربران و دستگاه‌ها در دامنه: هر کاربر و دستگاه برای پیوستن به یک دامنه، اطلاعات احراز اصالتی خود را به مرجع دامنه محلی ارسال کرده و مرجع بر اساس ویژگی‌ها، کلید عمومی و خصوصی، کلید جستجو را برای کاربران ایجاد و ارسال خواهد کرد. این اطلاعات در زنجیره اول و یک انباشتگر پویا ذخیره می‌گردد؛ بنابراین مراحل بعدی احراز اصالت سریع‌تر انجام می‌شود. همچنین یک آستانه برای دامنه در نظر گرفته تا ابطال دوگانه به‌موقع کاربران و ویژگی‌ها که دارای دوره هستند، انجام ی‌پذیرد. این اطلاعات در مرجع دامنه جهان جمع خواهد شد.

۲- احراز اصالت: احراز اصالت توسط مرجع دامنه محلی انجام می‌گیرد. هر موجودیت برای ثبت شدن در دامنه اطلاعات هویتی خود مانند نام، شناسه و ویژگی‌های خود را به مرجع ارسال کرده و مرجع پس از دریافت این اطلاعات منحصربه‌فرد، کاربر را معتبر شناخته و این اطلاعات ثبت می‌گردد. برای ثبت یک دستگاه نیز اطلاعات منحصربه‌فرد دستگاه مانند شناسه دستگاه، تاریخ و نام مالک به مرجع ارسال می‌گردد. سپس مرجع این اطلاعات را ثبت و دستگاه را معتبر شناسایی خواهد کرد. این اطلاعات در زنجیره



شکل (۳). معماری طرح پیشنهادی

معماری شامل موجودیت‌های زیر است:

۱) دامنه^۱: طرح شامل دامنه‌های مختلف است که در هر دامنه تعدادی کاربر و دستگاه مستقر شده است.

(۲) کاربر^۲: کاربر موجودیتی است که داده‌هایی را تولید و ذخیره کرده و همچنین مالک دستگاه است و درخواست دسترسی به داده‌ها از دامنه دیگر را می‌تواند داشته باشد. داده‌های خود را برای اشتراک‌گذاری در فضای ابری رمز و بارگذاری خواهد کرد.

(۳) دستگاه^۳: دستگاه‌هایی که در اینترنت اشیا قرار گرفته‌اند، قادر به تولید داده هستند.

۴) دروازه^۴: درخواست‌های دسترسی به داده‌ها توسط دروازه‌ها دریافت می‌شوند و فیلتر کردن درخواست مبتنی بر احراز اصالت توسط دروازه انجام می‌گیرد. یعنی فقط درخواست کاربران احراز شده پردازش شده و از لحاظ تازگی و مهر زمانی نیز درخواست بررسی و فیلتر می‌گردد؛ بنابراین همه درخواست‌ها پردازش نمی‌شوند؛ بلکه فقط درخواست تازه کاربران احراز شده بررسی خواهند شد.

(۵) سرورهای لبه^۵: درخواست‌های فیلتر شده به لبه ارسال می‌گردد. تفویض دسترسی توسط لبه انجام می‌پذیرد. با استفاده از بهینه‌سازی مجموعه‌ای از گره‌های نمایندگی بهینه از لحاظ بار، سطح انرژی، ارزش و اعتماد انتخاب می‌شود و سپس با اجماع Trusted PBFT از بین نمایندگان بهترین گره برای تفویض انتخاب می‌شود. سپس درخواست دریافتی همراه با ویژگی‌های کاربر توسط یک کانال برای دامنه هدف ارسال می‌گردد.

۶) مرجع دامنه محلی^۶: در هر دامنه یک مرجع محلی قرار گرفته است. کاربران و دستگاه‌ها برای ثبت شدن در دامنه

¹. Domain.

2. User.

³ Device⁴. GateWay.

5. Edge.

⁶. Local Domain Authentication.

⁷. Cloud node.⁸. Global Domain Authentication.

درخواست به همراه ویژگی و اطلاعات به لبه ارسال می‌شود. همچنین مالک داده یک ساختار دسترسی و مجموعه جهان ویژگی تعریف کرده و امکان جستجو برای کاربرانی که سیاست موجود در ساختار دسترسی را فراهم کنند ایجاد می‌کند و این امکان را به کاربر می‌دهد تا با فراخوانی قرارداد هوشمند و کلمه کلیدی از طریق یک دریاچه داده‌ای را جستجو کند.

۴- تفویض دسترسی و احراز اصالت متقابل دامنه‌ای: سرورهای لبه با دریافت اطلاعات از دروازه، دامنه هدف را شناسایی کرده و سپس با یک الگوریتم بهینه‌سازی یک مجموعه گره نمایندگی برای تفویض دسترسی ایجاد کرده، همچنین با استفاده از اجماع Trusted PBFT گره بهینه‌تر از نظر بار، سطح انرژی و ارزش و اعتبار برای تفویض دسترسی انتخاب می‌شود [۲]. سپس از طریق یک کانال، کانال ارتباطی بین لبه و لبه هدف ایجاد شده و درخواست به همراه ویژگی و کلید جستجو برای لبه هدف ارسال می‌گردد.

۵- جستجو مبتنی بر کلمه کلیدی و دریاچه: به کمک قراردادهای هوشمند، ساختار دسترسی و جستجو بر اساس ویژگی توسط مالک برای کاربران فراهم می‌گردد. یعنی اگر ویژگی‌های کاربر، ویژگی‌های موجود در سیاست ساختار دسترسی تعریف شده توسط مالک را برآورده کند، یک قرارداد برای جستجو برای او ایجاد می‌گردد و با استفاده از کلید جستجو تولید شده امکان ارسال درخواست مبتنی بر کلمه کلیدی برای کاربر فراهم می‌شود. قرارداد هوشمند از دریاچه و کلمه کلیدی برای جستجوی فایل رمزی استفاده می‌کند. بررسی صورت می‌گیرد که مجموعه ویژگی‌های این کاربر با سیاست دسترسی مطابقت دارد یا خیر. کاربر کلمه کلیدی را به دروازه ارسال کرده و دروازه آن را با درخواست به لبه ارسال می‌کند و این ویژگی به صورت یک دریاچه نمایش داده می‌شود.

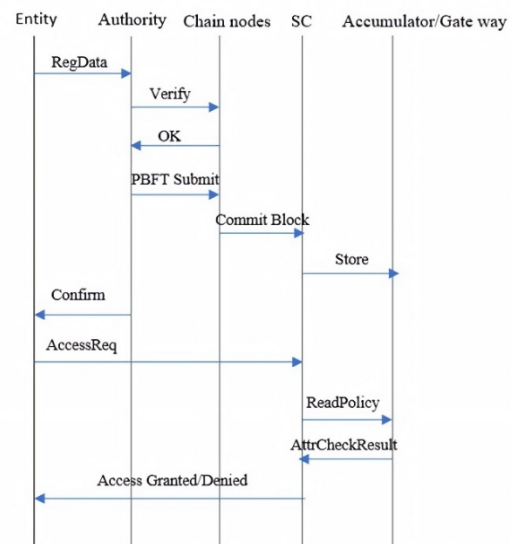
۶- رمزگشایی جزئی فایل بازیابی شده: دستگاه هدف پاسخ درخواست را به لبه ارسال و توسط لبه رمزگشایی جزئی بدون افشاشدن کلید انجام می‌گیرد. سپس پاسخ به کاربر ارسال می‌گردد. کاربر با کلید تأیید شده رمزگشایی را تکمیل کرده و فایل بازیابی می‌شود.

۷- رمزنگاری و رمزگشایی برخط و برون خط: رمزگشایی جزئی توسط سرورهای لبه انجام می‌گیرد و بار محاسباتی برای کاربران کاهش می‌یابد. پیش محاسبات به صورت برون خط انجام می‌شود تا سرعت افزایش یابد. تولید برخی از کلیدهای جزئی، کلیدهای احراز اصالت، امضا، تأیید امضا، دریافت اطلاعات هویتی از انباشتگر یا زنجیره اول و برقراری کانال می‌تواند به صورت برون خط انجام شود. اما بازیابی درخواست برخط صورت می‌گیرد.

۸- اشتراک گذاری اطلاعات: داده‌ها با ABSE توسط مالک رمز می‌شود. داده رمز شده به همراه سیاست دسترسی به این داده‌ها در

اول ذخیره شده و هر زمان که یک کاربر نخستین بار دسترسی به دستگاه دیگری را بخواهد، برای احراز اصالت به زنجیره مراجعه کرده و با اجماع احراز اصالت صورت می‌گیرد. مرجع این اطلاعات را در انباشتگر پویا نیز کپی کرده که همه موجودیت‌های یک دامنه به آن دسترسی دارند و گره‌های دروازه با استفاده از این اطلاعات فیلتر کردن درخواست‌ها را انجام خواهند داد.

مرحله احراز اصالت مشابه با کار انجام شده در مقاله [۶] دو قسمت می‌شود. همان‌طور که ذکر شد، اولین باری که دستگاه‌ها و کاربران می‌خواهند ثبت‌نام کنند، به زنجیره اول مراجعه کرده و توسط مرجع دامنه محلی با اجماع زنجیره ثبت می‌گردند. در مراحل بعدی برای احراز اصالت اطلاعات در انباشتگر پویا موجود است و نیاز نیست مجدد به زنجیره مراجعه شود. از انباشتگر با قرارداد هوشمند، هر زمان که نیاز به بررسی هویت باشد، سایر موجودیت‌های دامنه اطلاعات را دریافت و به صورت برون خط بررسی انجام می‌پذیرد و سرعت احراز اصالت و دوره‌های ارتباطی کاهش خواهند داشت؛ بنابراین زمانی که کاربر برای اولین بار درخواست دسترسی به داده‌ای را داشته، احراز اصالت با استفاده از زنجیره قالب و اجماع انجام خواهد شد؛ اما در مراحل بعد با مراجعه به انباشتگر و فراخوانی قرارداد هوشمند، اجماع دیگر انجام نمی‌پذیرد. به همین علت است که دوره‌های ارتباطی کاهش خواهند داشت [۶]. پروتکل شکل ۴ برای نشان دادن بهتر عملیات احراز اصالت توسط نویسنده طراحی گردیده است.



شکل (۴). پروتکل احراز اصالت و دسترسی

۳- درخواست دسترسی و فیلتراسیون درخواست: کاربر درخواست خود را به دروازه ارسال کرده و دروازه با استفاده از اطلاعات هویتی ثبت شده یک فیلتر درخواست مبتنی بر احراز اصالت انجام می‌دهد و درخواست‌ها از لحاظ تازگی و مهر زمانی بررسی می‌گردد؛ بنابراین همه درخواست‌ها پردازش نخواهند شد و سرعت ارسال درخواست افزایش خواهد یافت. سپس این

عمومی سیستم^۱ به عنوان خروجی ایجاد می شوند. پارامترهای عمومی شامل:

$$(e, G, G, G_T, g, p, E, \acute{E}, t_0, \{t_i\}_{i \in \{1, n\}}, H) \quad (1)$$

و همچنین کلید اصلی خصوصی به عنوان خروجی تولید می شود:

$$MSK = (\alpha, \beta) \quad (2)$$

ابتدا یک زوج سازی دوخطی تعریف می شود:

$$e: G \times G \rightarrow G_T \quad (3)$$

که G و G_T دو گروه ضربی با مولد g از مرتبه اول p در نظر گرفته می‌شوند.

سیپر، E و $\dot{E}$ محاسبه می شوند:

$$E = e(g, g)^\alpha \quad (4)$$

$$\dot{E} = e(q, q)^{\alpha\beta} \quad (\Delta)$$

جایی که $t_0, \alpha, \beta \in \mathbb{Z}_p$ به طور تصادفی انتخاب می‌شوند. یک تابع چکیده‌ساز مقاوم در برابر خورد انتخاب می‌شود:

$$H : \{0,1\}^* \rightarrow G \quad (6)$$

مجموعه جهان ویژگی تعریف می گردد:

$$A = \{a_1, \dots, a_n\} \quad (\forall)$$

و برای هر ویژگی $a_i \in A$ به طور تصادفی $t_i \in G$ انتخاب می‌شود.

راه‌اندازی: این الگوریتم توسط مرجع دامنه محلی اجرا می‌شود. پارامتر امنیتی λ به‌عنوان ورودی دریافت می‌شود و جفت کلید خصوصی/عمومی (MPK, MSK) به‌عنوان خروجی تولید می‌شود. در ادامه ویژگی‌های مجموعه S و کلید رمز MSK به‌عنوان ورودی دریافت می‌شوند و یک کلید رمز SK به‌عنوان خروجی ایجاد می‌شود. علاوه بر الگوریتم راه‌اندازی الگوریتم SKGen و OSKGen توسط مرجع فراخوان می‌شود.

توضیح الگوریتم SKGen:

این الگوریتم توسط مرجع دامنه محلی اجرا می‌شود. پارامتر عمومی سیستم، کلید اصلی خصوصی و ساختار دسترسی (M,P) لایه را به طوری که M ماتریس $m \times l$ و P یک تابع برجسب گذاری است که سطر k ام، MK ماتریس M را به ویژگی $\sigma\rho(k)$ مرتبط می‌سازد، به عنوان ورودی دریافت می‌شوند. سپس کلید مخفی توسط این الگوریتم تولید می‌شود:

$$SK(M, \rho) = ((M, \rho), B_{1,k}, B_{2,k}, \{B_{3,k,i}\}_{ai \in A \setminus \{\rho(k)\}}), \quad (\lambda)$$

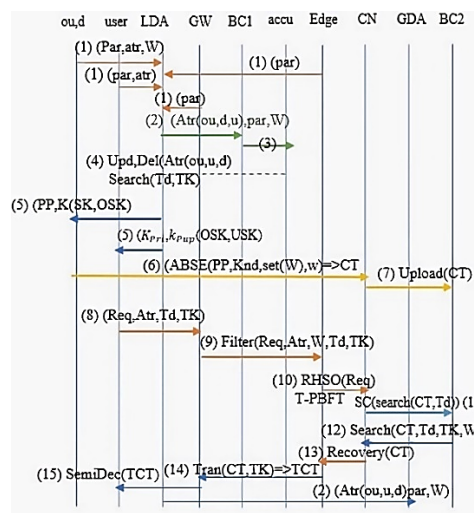
$$B_{4,k}, B_{5,k}, \{B_{6,k,i}\}_{ai \in A \setminus \{\rho(k)\}}) K \in \{1, m\}$$

ابر ذخیره می‌گردد. به همراه آن کلمه کلیدی لازم، ساختار دسترسی و جستجو نیز ذخیره می‌شوند. از داده‌ها یک چکیده گرفته می‌شود و در زنجیره دوم برای بررسی یکبارچگی ذخیره می‌گردد.

۹- ابطال دوگانه و کنترل دسترسی پویا: ابطال دوگانه بر اساس ابطال کاربران مخرب و ابطال ویژگی‌ها بر اساس زمان انقضا صورت می‌گیرد. کاربران مخرب بر اساس رفتار یا تحت‌تأثیر یک کاربر مخرب دیگر ارزش خود را از دست داده و زمانی که ارزش آن‌ها به زیر مقدار تعریف شده آستانه در دامنه برسد، از دامنه حذف می‌شوند و برای پیوستن، باید مجدد احراز اصالت شوند و کلید برای آن‌ها ایجاد گردد. برای هر ویژگی یک‌زمان انقضا در نظر گرفته می‌شود که پس از آن ویژگی باطل و به‌روزرسانی می‌شود.

۱۰- قرارداد هوشمند: قرارداد هوشمند قوانین از پیش نوشته شده‌ای تعریف می‌شوند که در زمان نیاز به طور خودکار راه‌اندازی می‌گردند. در این طرح قرارداد برای ایجاد دسترسی توسط مالک بر اساس سیاست دسترسی راه‌اندازی می‌شود. این قرارداد برای جستجو توسط کاربر با ویژگی دسترسی، برای یک درخواست فراخوانی می‌شود. برای حفظ عدالت و انصاف در دسترسی، برای برقراری حقوق یکسان درخواست‌های مختلف به داده‌ها، قرارداد به کار گرفته می‌شود. زمانی که کاربران برای مثال درخواست دسترسی به یک داده یکسان داشته باشند، قرارداد بر اساس اهمیت دسترسی تصمیم می‌گیرد چه کسی ابتدا دسترسی داشته باشد [۳].

[۴]. قرارداد برای استفاده از انباشتگر پویا توسط مرجع دامنه محلی راه‌اندازی می‌شود تا موجودیت‌ها برای احراز اصالت سایر اجزا آن را فراخوانی کنند [۶]. جزئیات قرارداد هوشمند، به علت محدودیت مقاله طبق، [۲]، [۳]، [۴]، [۶] آورده نشده‌اند.



شکل (۵). گردش کار طرح پیشنهادی

(۱) راه اندازی اولیه سیستم (ثبت نام کاربران و دستگاه‌ها):

الگوریتم راه اندازی توسط مرجع دامنه محلی اجرا می شود. با دریافت پارامتر امنیتی سیستم به عنوان ورودی، پارامترهای

¹. Public parameter.

$$\hat{B}_{5,k} = (B_{5,k})^u = g^{ur_k} \quad (26)$$

$$\{\hat{B}_{6,k,i} = (B_{6,k,i})^u = t_i^{ur_k}\}_{ai \in A \setminus \{\rho(k)\}} \quad (27)$$

۲ ذخیره اطلاعات در زنجیره قالب اول و انباشتگر پویا

پس از ارسال اطلاعات توسط موجودیت‌ها به مرجع دامنه محلی، این اطلاعات در زنجیره قالب ثبت می‌گردد و برای احراز اصالت موجودیت‌ها و تولید کلید دسترسی مورد استفاده قرار می‌گیرد [۲]. اطلاعات ثبت شده در یک انباشتگر نیز ذخیره می‌گردد، همان‌طور که قبلاً نیز اشاره شد این اطلاعات به‌صورت تجمیعی برای افزایش سرعت در مراحل بعدی ذخیره می‌شوند [۶].

۲-۱ ثبت اطلاعات مراجع دامنه محلی در مرجع دامنه جهانی

در هر دامنه یک مرجع محلی مستقر شده است که اطلاعات و پارامترهای موجودیت هر دامنه را محلی نگهداری می‌کند. همچنین یک مرجع دامنه جهانی در فضای ابری قرار داده شده است که اطلاعات مراجع محلی را تجمیع و ذخیره می‌نماید و امکان برقراری و بررسی احراز اصالت بین دامنه‌ای توسط آن فراهم می‌گردد [۲].

۳ ذخیره اطلاعات در انباشتگر پویا

انباشتگر پویا از طریق قرارداد هوشمند در زنجیره اول در دسترس قرار داده می‌گیرد [۴]. اطلاعات احراز اصالت و جستجو در آن تجمیع می‌گردد و در مراحل بعدی برای کاهش تأخیر دسترسی مورد استفاده قرار می‌گیرد. اطلاعات تجمیع شده در انباشتگر قابل حذف، به‌روزرسانی و تأیید نیز خواهد بود. برای دسترسی یک دستگاه به دستگاه دیگر در دامنه‌ای متفاوت، احراز اصالت باید انجام شود. اطلاعات احراز اصالت توسط مرجع دامنه دریافت شده و در زنجیره اول و انباشتگر ذخیره می‌گردد. در احراز اصالت‌های بعدی از قرارداد هوشمند و انباشتگر استفاده می‌شود [۶]. احراز اصالت در دو مرحله انجام می‌پذیرد. مرحله پیش احراز اصالت در زمان ثبت دستگاه و اطلاعات توسط زنجیره و در مراحل بعدی با انباشتگر صورت می‌پذیرد.

۴ حذف، به‌روزرسانی و عملیات تأیید داده به کمک انباشتگر

افزودن داده در انباشتگر پویا:

در این مرحله اطلاعات لازم برای دستگاه توسط لبه تولید می‌شود و به مرجع دامنه محلی ارسال می‌گردد. سپس این اطلاعات در ترکیب با قراردادهای هوشمند و فناوری انباشت‌کننده پویا برای عملیات احراز اصالت سریع بعدی در زنجیره قالب اول توسط مرجع بارگذاری می‌گردد. برای جزئیات بیشتر از نحوه کار انباشتگر و فراخوانی قرارداد هوشمند به مقاله [۶] می‌توان مراجعه کرد.

سپس به کمک الگوریتم مقادیر زیر محاسبه می‌شود:

$$\sigma\rho(k) = MK.V \quad (9)$$

جایی که بردار V به‌صورت زیر تعریف می‌شود:

$$V = (\alpha, V_2, \dots, V_1) \quad (10)$$

و برآورده می‌شود:

$$(1, 0, \dots, 0) = a \quad (11)$$

سپس در ادامه به طور تصادفی r_k و $\hat{r}_k$ به‌صورت زیر انتخاب می‌شوند:

$$r_k, \hat{r}_k \in Zp \quad k \in [1, m] \quad (12)$$

سپس محاسبات زیر انجام می‌شود:

$$B_{1,k} = g^{\sigma\rho(k)}(t_0 \ t_{\rho(k)})^{r_k} \quad (13)$$

$$B_{2,k} = g^{r_k} \quad (14)$$

$$\{B_{3,k,i} = t_i^{r_k}\}_{ai \in A \setminus \{\rho(k)\}} \quad (15)$$

$$B_{4,k} = g^{\sigma\rho(k)}(t_0 \ t_{\rho(k)})^{\hat{r}_k} \quad (16)$$

$$B_{5,k} = g^{\hat{r}_k} \quad (17)$$

$$\{B_{6,k,i} = t_i^{\hat{r}_k}\}_{ai \in A \setminus \{\rho(k)\}} \quad (18)$$

توضیح الگوریتم OSKGen:

این الگوریتم توسط مرجع دامنه محلی برای تولید کلید برون‌سپاری مورد استفاده قرار می‌گیرد. کلید اصلی خصوصی، پارامترهای عمومی سیستم، کلید خصوصی بر اساس ساختار دسترسی به‌عنوان ورودی دریافت می‌شود و به طور تصادفی u انتخاب می‌گردد. که:

$$u \in Zp \quad USK = u \quad (19)$$

سپس کلید برون‌سپاری محاسبه می‌شود:

$$OSK(M, \rho) = ((M, \rho), \hat{B}_0, \hat{B}_{1,k}, \hat{B}_{2,k}, \{ \hat{B}_{3,k,i} \}_{ai \in A \setminus \{\rho(k)\}}, \hat{B}_{4,k}, \hat{B}_{5,k}, \{ \hat{B}_{6,k,i} \}_{ai \in A \setminus \{\rho(k)\}}, k \in [1, m]) \quad (20)$$

محاسبات زیر صورت می‌گیرد:

$$\hat{B}_0 = g^{\alpha(\beta-u)} \quad (21)$$

$$\hat{B}_{1,k}(B_{1,k})^u = g^{u\delta\rho(k)}(t_0 \ t_{\rho(k)})^{ur_k} \quad (22)$$

$$\hat{B}_{2,k} = (B_{2,k})^u = g^{ur_k} \quad (23)$$

$$\{\hat{B}_{3,k,i} = (B_{3,k,i})^u = t_i^{ur_k}\}_{ai \in A \setminus \{\rho(k)\}} \quad (24)$$

$$\hat{B}_{4,k} = (B_{4,k})^u = g^{u\delta\rho(k)}(t_0 \ t_{\rho(k)})^{ur_k} \quad (25)$$

۵) ارسال کلید برای موجودیت‌های احراز شده توسط مرجع دامنه محلی

کلید مربوطه توسط مرجع دامنه محلی برای موجودیت‌هایی که احراز اصالت شده‌اند، توسط مرجع دامنه محلی ارسال می‌گردد.

۶) رمزنگاری

مالک داده از کلید عمومی خود PK برای رمزگذاری متن ساده، چکیده‌ساز و مجموعه ویژگی مربوطه W استفاده می‌کند. سپس، داده‌های رمز شده توسط مالک در ابر بارگذاری می‌شوند. متن رمزی CT در بلاک زنجیره ذخیره می‌گردد تا توزیع و ذخیره‌سازی قابل‌اعتماد داده تضمین شود [۵].

توضیح الگوریتم رمزنگاری:

این الگوریتم برای رمزگذاری داده‌ها توسط مالک مورد استفاده قرار می‌گیرد. پارامترهای عمومی سیستم، مجموعه جهانی W که تعریف شده، کلمه کلیدی w و متن ساده به‌عنوان ورودی دریافت می‌گردد. سپس یک مقدار مخفی S به‌صورت تصادفی از مجموعه Z_p انتخاب می‌شود به‌طوری‌که:

$$s \in Z_p \quad (28)$$

سپس متن رمزی محاسبه می‌شود که متن رمزی شامل:

$$CT = (W, C_1, C_2, C_3, C_4) \quad (29)$$

همچنین:

$$C_1 = \text{Msg}.E^S \quad (30)$$

$$C_2 = g^S \quad (31)$$

$$C_3 = (t_0 \prod_{a \in W} t_i) \quad (32)$$

$$C_4 = \hat{E}^S.e(g^S, H(w)) \quad (33)$$

۷) ذخیره داده‌های رمز شده در زنجیره

پس از رمزنگاری داده‌ها به همراه خط مشی دسترسی با استفاده از رمزنگاری مبتنی بر ویژگی توسط مالک، این داده‌ها در فضای ابری به همراه کلید و ساختار دسترسی، بارگذاری می‌شوند تا کاربرانی که اجازه رمزگشایی دارند مشخص شوند. یک نسخه از داده‌ها رمز شده در زنجیره دوم که به فضای ابری دسترسی دارد و از قرارداد هوشمند برای جستجو بهره می‌گیرد، ذخیره می‌گردد [۵].

سپس یک نسخه چکیده از این داده‌ها گرفته شده و در زنجیره ذخیره می‌گردد. امکان جستجو مبتنی بر کلمه کلیدی در زنجیره دوم توسط قرارداد هوشمند فراهم می‌گردد. همچنین عدالت و انصاف در دسترسی به داده‌ها تضمین می‌شود [۳] و با استفاده از چکیده، یکپارچگی داده‌ها نیز قابل‌بررسی است [۴].

۸) ارسال درخواست دسترسی به داده

درخواست دسترسی به داده موجود در دامنه دیگر توسط کاربر به دروازه ارسال می‌شود. دروازه با استفاده از اطلاعات احراز اصالتی ذخیره شده در زنجیره اول فیلتر درخواست مبتنی بر احراز اصالت، تازگی پیام بر اساس مهر زمانی و غیرتکراری بودن را انجام می‌دهد [۲]. سپس درخواست فیلتر شده برای تفویض دسترسی به گره‌های لبه ارسال می‌شود.

۹) فیلتراسیون درخواست مبتنی بر احراز هویت

دسترسی هم‌زمان توسط کاربران به دستگاه اینترنت اشیا توسط دروازه به گره لبه ارسال می‌شود که باعث کاهش حملات انکار سرویس^۱ می‌شود. تأیید صحت درخواست‌ها توسط دروازه با فیلتر انجام می‌پذیرد. فیلتر درخواست با آرایه خالی m بیت انجام می‌شود. عنصر برای عضویت در فیلتر باید تأیید شود و سپس false برمی‌گردد. برای افزودن یک عنصر به فیلتر، چکیده SHA-256 پذیرفته می‌شود. از نتیجه چکیده برای گرفتن موقعیت در آرایه استفاده می‌شود. هر موقعیت از آرایه به یک عنصر تخصیص داده می‌شود. از چکیده برای ایجاد موقعیت‌های موجود در فیلتر استفاده می‌شود. سپس قانونی بودن درخواست از طریق آن تأیید می‌گردد.

در ادامه، درخواست دسترسی به داده توسط کاربر ارسال می‌شود. برای این منظور، ابتدا از کلید خصوصی که برای کاربر ایجاد شده، برای ساختن یک دريچه استفاده می‌شود که این دريچه بر اساس کلید مبتنی بر ویژگی توسط مرجع دامنه محلی ساخته می‌شود. برای این منظور از الگوریتم TdGen استفاده می‌شود. سپس درخواست فیلتر و به گره‌های لبه فرستاده می‌شود. همچنین یک کلید تبدیل نیز تولید می‌شود تا با استفاده از آن متن رمزی نیمه رمزگشایی شده را کاربر به دست بیاورد. این کلید با TkGen ایجاد می‌شود. کلید دريچه و کلید تبدیل به لبه ارسال می‌شوند. قرارداد هوشمند از دريچه برای جستجوی بلوک داده استفاده می‌کند و بررسی می‌شود که مجموعه ویژگی W متن رمزی با ساختار دسترسی LSSS درخواست‌کننده مطابقت دارد یا خیر. پس از تأیید معتبر بودن نتیجه جستجوی داده، الگوریتم رمزگشایی جزئی Tran اجرا می‌شود و متن رمزی جزئی تولید شده TCT برای کاربر ارسال می‌گردد. در همان زمان، داده‌های مرتبط با درخواست و فرایند جستجو در زنجیره دوم نوشته می‌شوند تا شواهد غیرقابل‌انکار برای اثبات صحت اشتراک‌گذاری فراهم گردد [۵].

توضیح الگوریتم TdGen:

این الگوریتم توسط کاربری که درخواست دسترسی به داده‌ای را دارد اجرا می‌شود. کاربر با استفاده از کلید خود و ویژگی‌های لازم، دريچه برای دسترسی به داده را با الگوریتم می‌سازد. کلید

^۱. DDOS.

سطح انرژی: برای تعیین سطح انرژی فعلی گره استفاده می‌شود. هرچه سطح انرژی گره بالاتر باشد، برای یک تفویض کننده، تبدیل به نماینده بهینه برای تفویض دسترسی می‌شود.

$$E = \xi - \varepsilon \quad (44)$$

بار: هرچه بار یک گره کمتر باشد، به‌عنوان نماینده بهینه انتخاب می‌شود.

$$L = \sum_{i=1}^n w_n \quad (45)$$

منابع در دسترس: گره‌ای که منابع بیشتری در اختیار داشته باشد، به‌عنوان نماینده بهینه برای تفویض دسترسی انتخاب می‌شود.

$$RA = \eta - \zeta \quad (46)$$

۸-۱) جستجو متن رمزی

قرارداد هوشمند، دریچه Td را برای جستجوی بلوک داده مورد استفاده قرار می‌دهد و تطابق بین مجموعه ویژگی W در متن رمزی با ساختار دسترسی LSSS کاربر درخواست کننده بررسی می‌شود. پس از تأیید معتبر بودن نتیجه جستجوی داده، الگوریتم رمزگشایی جزئی Tran اجرا می‌شود و متن رمزی جزئی تولید شده TCT برای کاربر ارسال می‌گردد. در همان زمان، اطلاعات مربوط به رکورد درخواست و فرایند جستجو در زنجیره دوم ثبت می‌شود [۵].

۸-۲) حالت جستجو

در این مرحله، جستجو متن رمزی با استفاده از تطبیق فهرست متن رمزی و دریچه توسط SE پیاده‌سازی می‌گردد. فرایند جستجو، با دریافت کلمات کلیدی از کاربران و ارسال به سرور لبه به‌صورت دریچه نمایش داده می‌شود. جستجو درشت‌دانه و ریزدانه مبتنی بر ساختار دسترسی، با فیلتر کردن اطلاعات کاربران انجام می‌پذیرد [۵]. امنیت و دشواری کلیدواژه بر اساس BDH ثابت می‌گردد. در ادامه، قرارداد هوشمند با تطبیق دریچه و شاخص کلید، جستجوی متن رمزی حاوی کلمه کلیدی را اجرا می‌کند. دریچه غیر قابل پیوند است یعنی، دریچه‌هایی که توسط کاربران مختلف برای یک کلمه تولید می‌شوند، متفاوت است. متن‌های رمزی که کلمات کلیدی آن‌ها ساختار دسترسی را برآورده می‌کنند، شناسایی شده و بازایی می‌شوند. متن رمزی دارای یک ساختار دسترسی است و کاربری که آن را برآورده کرده بر اساس کلمه کلیدی، می‌تواند آن را رمزگشایی کند. این عملیات جستجو توسط قرارداد هوشمند صورت می‌پذیرد.

۱۱) بازایی داده‌ها:

برای بازایی داده‌ها، از پارامتر عمومی، متن رمزی و کلید تبدیل استفاده می‌شود. مجموعه‌ای از ثابت‌ها تولید می‌شوند که ساختار دسترسی را ارضا نمایند. این الگوریتم توسط کاربر برای جستجو متن رمزی بر اساس کلمه کلیدی و از

OSK، درخواست کاربر که به‌صورت یک کوئری نمایش داده می‌شود، به‌عنوان ورودی توسط الگوریتم دریافت می‌شود. سپس محاسبات زیر را برای ساختن دریچه اجرا می‌شود:

$$T_0 = \hat{B}_0 \cdot H(q) \quad (34)$$

$$T_1 = \hat{B}_{4,k} \quad (35)$$

$$T_2 = \hat{B}_{5,k} \quad (36)$$

$$T_3 = \hat{B}_{6,k,i} \quad (37)$$

خروجی الگوریتم برابر است با:

$$TD = (T_0, T_1, T_2, T_3) \quad (38)$$

توضیح الگوریتم TKGen:

این الگوریتم توسط لبه برای ایجاد کلید تبدیل استفاده می‌شود. این کلید توسط سرور لبه برای رمزگشایی جزئی متن رمزی در مراحل بعدی استفاده می‌شود. الگوریتم کلید برون‌سپاری OSK را به‌عنوان ورودی دریافت کرده و محاسبات زیر انجام می‌پذیرد:

$$TK_1 = \hat{B}_{1,k} \quad (39)$$

$$TK_2 = \hat{B}_{2,k} \quad (40)$$

$$TK_3 = \hat{B}_{3,k,i} \quad (41)$$

خروجی الگوریتم کلید تبدیل است که:

$$TK = ((M, \rho), TK_1, TK_2, TK_3) \quad (42)$$

۱۰) بهینه‌سازی RHSO و اجماع T-PBFT

نمایندگی دسترسی مبتنی بر اعتماد:

درخواست فیلتر شده به لبه ارسال می‌گردد. گره‌های لبه باید تفویض دسترسی را فراهم کنند. به‌منظور انتخاب نماینده مناسب، یک مجموعه نمایندگی به کمک زنجیره ایجاد می‌شود و با بهره‌گیری از الگوریتم RHSO گره نماینده انتخاب می‌گردد. فرایند انتخاب نماینده بهینه، بر اساس الگوریتم بهینه‌سازی با در نظر گرفتن پارامترهایی نظیر ارزش اعتماد^۱، سطح انرژی^۲، بار^۳، منابع در دسترس^۴ صورت می‌گیرد. براین اساس رهبران و پیروان مقداره‌ی اولیه می‌شوند. رهبر که بر فعالیت پیروان نظارت دارد، به‌عنوان بهترین گره تشخیص داده می‌شود و برای انتخاب نماینده بهینه مورد استفاده قرار می‌گیرد.

ارزش اعتماد: بر اساس گره‌های همسایه در شبکه محاسبه می‌شود.

$$T = \sum_{i=1}^n F_n \quad (43)$$

¹. Trusted value.

². Energy level.

³. Load level.

⁴. Resources Availability.

$$TCT = \frac{e(C_3, \prod_{k \in K} (\hat{B}_{2,k})^{\tau k})}{e(C_2, \prod_{ai \in W \setminus \{\rho(k)\}} \hat{B}_{3,k,i})^{\tau k}} \quad (53)$$

اگر برآورده نکند، اجرای الگوریتم متوقف می‌شود.

تکمیل رمزگشایی:

کاربر پس از دریافت متن رمزی نیمه رمزگشایی شده با استفاده از کلید خصوصی، رمزگشایی را با اجرای الگوریتم Dec تکمیل کرده و داده بازیابی می‌شود. صحت و کامل بودن نتیجه، با مقایسه متن ساده بازیابی شده و چکیده آن اعتبارسنجی می‌شود.

توضیح الگوریتم Dec:

این الگوریتم برای رمزگشایی متن نیمه رمزگشایی شده توسط کاربر مجاز به کار می‌رود. متن رمزی تبدیل شده C_1 و کلید خصوصی USK به عنوان ورودی دریافت می‌شود و متن اصلی بازیابی می‌گردد.

$$Knd = C_1 \cdot TCT^{\frac{1}{u}} \quad (54)$$

۱۳ قرارداد هوشمند (عدالت و انصاف - انباشتگر - توکن دسترسی و توکن جستجو)

برای دسترسی و جستجو توسط مالک به کاربر، از قرارداد هوشمند توسط زنجیره قالب دوم متصل به سرور ابری استفاده می‌شود [۷]. با اولین درخواست و ثبت نام، اطلاعات احراز اصالت در زنجیره اول و در انباشتگر ذخیره می‌گردد. برای مراحل بعدی زمانی که درخواستی به زنجیره دوم برای بازیابی داده رمز شده در ابر ارسال شود، برای احراز اصالت از اطلاعات انباشتگر استفاده می‌شود و نیازی به اجماع برای تأیید نیست. همچنین برای عدالت و انصاف در دسترسی به داده‌ها هنگام درخواست‌های هم‌زمان از قرارداد هوشمند استفاده می‌شود. جزئیات بیشتر در مورد قرارداد هوشمند در مراجع [۳ و ۷] آورده شده است.

۱۴ ابطال دوگانه

فرایند ابطال به صورت دوره‌ای بر اساس رفتار و ویژگی‌ها انجام می‌گیرد. در صورت شناسایی کاربر به عنوان مخرب یا انقضای ویژگی، دسترسی لغو می‌گردد و امکان بارگذاری داده در ابراز بین می‌رود. در صورتی که ویژگی باطل شود، درخواست مجدد به مرجع محلی ارسال می‌شود و کلید جدید تولید می‌گردد. صحت ویژگی جدید از طریق زنجیره تأیید می‌شود. در صورتی که مقدار اعتماد کاربری به زیر آستانه مشخص شده برسد، از دامنه حذف خواهد شد. این آستانه توسط مرجع محلی بر اساس آنتروپی شانن تعیین می‌گردد [۲].

$$H(T) = - \sum_{i=1}^n P(T_i) \log P(T_i) \quad (55)$$

H مقدار آستانه و T ارزش اعتماد کاربر است. آستانه کمتر از ۵/ شود، کاربر لغو می‌شود.

طریق فراخوانی قرارداد هوشمند اجرا می‌گردد. پارامترهای عمومی سیستم، متن رمزی و دریچه ایجاد شده توسط الگوریتم TDGen به عنوان ورودی دریافت می‌شود. در نهایت متن رمز تبدیل شده محاسبه و ارائه می‌گردد [۵].

توضیح الگوریتم جستجو:

این الگوریتم توسط کاربر برای جستجو متن رمزی مبتنی بر کلمه کلیدی با فراخوانی قرارداد هوشمند اجرا می‌شود. پارامترهای عمومی سیستم، متن رمزی و دریچه ایجاد شده توسط الگوریتم TDGen به عنوان ورودی دریافت می‌شود. ابتدا مجموعه‌ای از ثابت‌ها ایجاد می‌شود:

$$\{v_k\} \in Zp \quad (47)$$

که عبارت زیر باید برآورده شود:

$$\sum_{k \in K} \delta \rho(k) \cdot v_k = (1, 0, \dots, 0) \quad (48)$$

جایی که در آن k مجموعه‌ای از همه K راضی کننده عبارت زیر را نشان می‌دهد:

$$\rho(k) \in W \quad (49)$$

مرحله تأیید: اگر معادله زیر برقرار باشد که به معنای وجود $q=W$ است، متن رمز شده برای کاربر ارسال می‌گردد. در غیر این صورت، جستجو با شکست مواجه شده و الگوریتم خروجی ۱ را می‌دهد.

$$\frac{e(C_2, T_0 \cdot \prod_{k \in K} (T_1 \cdot \prod_{ai \in A \setminus \{\rho(k)\}} T_3)^{V_k})}{e(C_3, \prod_{ai \in W} T_2^{V_k})} = C_4 \quad (50)$$

خروجی و متن رمز تبدیل شده محاسبه می‌گردد [۵].

۱۲ رمزگشایی جزئی داده بازیابی شده:

متن رمزی و رمزگشایی تبدیل شده TCT و USK بازیابی می‌شود [۵].

توضیح الگوریتم Tran:

این الگوریتم برای رمزگشایی جزئی متن رمزی، توسط سرورهای لبه اجرا می‌شود. متن رمزی بازیابی شده و کلید تبدیل TK تولید شده توسط الگوریتم TKGen به عنوان ورودی دریافت می‌شود و مراحل زیر را اجرا می‌گردد. ابتدا بررسی می‌شود که مجموعه ویژگی W متن رمزی، ساختار دسترسی (M,P) را برآورده می‌کند یا خیر. در صورت تأیید، مراحل زیر انجام می‌گیرد:

مجموعه‌ای از ثابت‌ها تولید می‌شود:

$$\{\tau k\} \in Zp \quad (51)$$

که عبارت زیر برآورده می‌شود:

$$\sum_{k \in K} \delta p(k) \cdot \tau k = (1, 0, \dots, 0) \quad (52)$$

سپس متن رمزی تبدیل شده TCT را محاسبه می‌گردد:

۳-۳. ویژگی‌های طرح پیشنهادی

در طرح پیشنهادی که برگرفته از طرح مقاله [۲] است، احراز اصالت متقابل دامنه‌ای، به کمک مراجع دامنه محلی و زنجیره قالب و انباشتگر صورت می‌پذیرد. باتوجه به اینکه یک چکیده از تمام تراکنش‌های درون شبکه تهیه شده و در زنجیره دوم متصل به فضای ابری ذخیره می‌شود، امکان بررسی سازگاری فراهم می‌گردد. تمامی داده‌ها در فضای ابری و زنجیره ذخیره شده و غیرقابل تغییر باقی می‌مانند؛ بنابراین به شواهدی غیرقابل انکار تبدیل می‌شوند. ابطال دوگانه کاربران بر اساس رفتار مخرب و ابطال ویژگی‌ها بر اساس زمان انقضا انجام می‌گیرد. داده‌ها با استفاده از رمزنگاری مبتنی بر ویژگی در فضای ابری بارگذاری می‌گردند، و حریم خصوصی و امنیت آن‌ها حفظ شده و امکان اشتراک‌گذاری بین دامنه‌ای به کمک ابر فراهم می‌شود. به دلیل استفاده از انباشتگر پویا، دوره‌های ارتباطی کاهش یافته و اطلاعات احراز اصالت ذخیره شده در آن، قابلیت به‌روزرسانی و حذف دارند. برخی از عملیات به‌صورت برون خط انجام‌پذیر است. رمزگشایی جزئی داده‌ها توسط سرورهای به‌صورت می‌گیرد. حریم خصوصی از طریق رمزنگاری مبتنی بر ویژگی تضمین می‌شود. استفاده از زنجیره قالب امکان ردیابی اطلاعات در هر زمان را فراهم می‌آورد. با به‌کارگیری اجماع PBFT و بهینه‌سازی، مقیاس‌پذیری سیستم فراهم شده است. استفاده از نام مستعار موجب ناشناس ماندن کاربران می‌شود. فیلترکردن مبتنی بر احراز اصالت از طریق دروازه‌ها از حملات انکار سرویس جلوگیری می‌کند. همچنین با بررسی تازگی درخواست‌ها از طریق مهر زمانی، از حملات تکراری پیشگیری می‌شود. با استفاده از رمزنگاری مبتنی بر کلمه کلیدی جستجو از طریق درپچه‌ها امکان پذیر می‌شود. ویژگی‌های طرح پیشنهادی با استناد به مقاله [۲]، [۵] و [۶] قابل اثبات است. جدول ۲ مقایسه کلی بین طرح‌های استفاده شده و طرح پیشنهادی را نشان می‌دهد.

جدول (۲). مقایسه طرح پیشنهادی با سایر طرح‌ها

نام طرح ویژگی	[۲]	[۴]	[۵]	[۶]	[۷]	[۸]	طرح پیشنهادی
احراز اصالت	✓	✓	✓	✓	✓	✓	✓
سازگاری	✓	✓	✓	✓	✓	✓	✓
عدم انکار	✓	✓	✓	✓	✓	✓	✓
ابطال دوگانه	✓	X	X	X	X	X	✓

اشتراک‌گذاری	✓	✓	✓	✓	✓	✓	✓
رمزگشایی جزئی برخط و برون خط	X	✓	✓	✓	✓	X	✓
کاهش دور ارتباطی	X	✓	✓	X	✓	X	✓
به‌روزرسانی سریع	✓	✓	✓	✓	✓	✓	✓
حریم خصوصی	✓	✓	✓	✓	✓	✓	✓
قابلیت ردیابی	✓	✓	✓	✓	✓	✓	✓
مقیاس پذیری	✓	✓	✓	✓	✓	✓	✓
ناشناس بودن	✓	✓	✓	✓	✓	✓	✓
فیلتر درخواست	✓	X	X	X	X	X	✓
جستجو	X	✓	✓	X	✓	X	✓
عدالت و انصاف	X	X	X	X	X	X	✓
انباشتگر پویا	X	X	✓	X	X	X	✓

طرح ارائه شده در مقاله [۲] با اعمال تغییراتی بر اساس سه منبع کلیدی بهبود یافته است. به همین منظور از انباشتگر پویا با استناد به مقاله [۶] قابلیت جستجو مبتنی بر کلمه کلیدی مطابق مقاله [۵] و استفاده هم‌زمان از دوزنجیره قالب مستقل بر اساس ساختار ارائه شده در مقاله [۴] بهره گرفته شده است. احراز اصالت متقابل دامنه‌ای با ارجاع به سازوکارهای مطرح شده در مقاله [۲] قابل استناد است.

- احراز اصالت متقابل: در این فرایند مراجع محلی در هر دامنه، مسئول دریافت ویژگی‌های منحصر به فرد کاربران و دستگاه‌ها هستند. این ویژگی‌ها پس از استخراج در زنجیره قالب ذخیره شده و در مراحل بعدی برای احراز

جدول (۳). پیچیدگی ذخیره‌سازی در طرح پیشنهادی

Explanation	Storage size	Component
اندازه رمز دانش متناسب با اندازه دانش متنی است به تعداد ویژگی‌ها وابسته نیست.	$O(Knd)$	Ciphertext (CT)
افزایش خطی با تعداد ویژگی‌های کلیدواژه کاربر	$O(n)$ elements in G	Trapdoor (Td)
وابسته به تعداد ویژگی‌های ساختار دسترسی کاربر	$O(m)$ elements in G_T	Conversion Key (TK)
شامل ترکیبی از ضرایب دسترسی، تصادفی‌ها و توابع چکیده	$O(m)$ elements in G and Z_p	Secret Key (SK)
بستگی به تعداد کلمات کلیدی ذخیره شده دارد	$O(W)$	Index for Keywords
جهت تأیید صحت پس از رمزگشایی استفاده می‌شود	Fixed (e.g 256 bits)	Abstract/Digest

جدول (۴). پیچیدگی هزینه محاسباتی طرح پیشنهادی

Notes	Computational Cost	Operation
تولید $E = e(g, g)^\alpha$ $\hat{E} = e(g, g)^{\alpha\beta}$ تولید پارامترهای عمومی	2 pairing operations + $O(n)$ exp.	Setup
وابسته به تعداد ویژگی‌های مرتبط با دانش	$O(1)$ + pairing + $O(W)$ exp	Encryption
هزینه سبک، سایر محاسبات به لبه واگذار می‌شود	2 exponentiations over G	TdGen (Trapdoor Gen)
ایجاد کلید تبدیل برای رمزگشایی جزئی	$O(m)$ exp. Over G_T	TKGen (Conv.KeyGen)
روی سرور لبه انجام می‌شود بدون افشا داده	2 pairing + 2 exp + multiplications	Tran (Partial Dec)
$Knd = C_1 \cdot TCT^{\frac{1}{\beta}}$ در سمت کاربر انجام می‌شود	1 multiplication + 1 inverse op	Dec (user dec)
با Td فقط تطبیق شاخص روی سرور انجام می‌شود، سبک است	$O(W)$ hash + equality checks	Search (SC match)

اصالت مورد استفاده قرار می‌گیرند. از آنجا که گره‌های دروازه به زنجیره قالب دسترسی دارند و عملیات فیلتر درخواست‌ها را نیز انجام می‌دهند، امکان احراز اصالت متقابل دامنه‌ای را برقرار می‌کنند.

- سازگاری و عدم انکار: استفاده از زنجیره قالب به دلیل ویژگی‌هایی نظیر سازگاری، ردیابی، غیرقابل انکار بودن تراکنش‌ها، باعث افزایش اعتماد سیستم می‌شود.
- ابطال دوگانه: ابطال دوگانه کاربران، بر پایه رفتارهای مخرب و انقضای ویژگی‌ها، طبق ساختار پیشنهادی در مقاله [۲] پیاده‌سازی شده است.
- اشتراک‌گذاری اطلاعات: بهره‌گیری از فضای ذخیره‌سازی ابری، بار محاسباتی سیستم را کاهش داده و امکان اشتراک‌گذاری امن و توزیع شده داده‌ها میان دامنه‌های مختلف را فراهم می‌سازد.
- کاهش دوره‌های ارتباطی: افزوده شدن انباشتگر پویا موجب کاهش دوره‌های ارتباطی شده و با وجود آن که طراحی دقیق این سازوکار در محدوده این نوشتار قرار ندارد، اعتبار آن با استناد به مقاله [۶] قابل تأیید است.
- حریم خصوصی: زنجیره قالب به دلیل قابلیت‌هایی چون ذخیره‌سازی تمامی تراکنش‌های شبکه، ویژگی‌های غیرقابل تغییر بودن، حریم خصوصی مناسبی را فراهم می‌نماید.
- مقیاس‌پذیری: مقیاس‌پذیری سیستم به کمک ترکیب دوزنجیره مستقل و استفاده از انباشتگر پویا ارتقا یافته است. چرا که می‌توان فرایندهای احراز اصالت و بررسی یکپارچگی را به صورت موازی مدیریت نمود.
- فیلتر شدن درخواست‌ها توسط گره‌های دروازه از بروز حملات انکار سرویس و تکرار جلوگیری به عمل می‌آورد که طبق مقاله [۲] قابل اثبات است.
- جستجو: با استفاده از مکانیزم جستجوی مبتنی بر کلمه کلیدی مطابق با مقاله [۵] کاربران می‌توانند به صورت سریع و دقیق به داده‌های مورد نظر دسترسی پیدا کنند. در این روش، کاربران با ساخت درجه‌هایی بر اساس ویژگی‌های خود، فرایند بازیابی داده را با دقت بالا انجام می‌دهند.
- در نتیجه، طرح پیشنهادی با افزودن قابلیت جستجوی کلمه کلیدی، انباشتگر پویا، بهره‌گیری از دوزنجیره قالب مستقل ساختار پایه معرفی شده در مقاله [۲] را توسعه داده است.

۴-۳ مقایسه طرح با طرح‌های گذشته

برای مقایسه و درک کارآمدی طرح، طرح پیشنهادی با دو مقاله [۷] [۸] که شباهت بیشتری به طرح دارد، مقایسه می‌گردد. ابتدا از لحاظ سربار ذخیره‌سازی طرح پیشنهادی در جدول ۳، سربار محاسباتی در جدول ۴، ارائه می‌گردد. سپس در جدول ۵ مقایسه طرح‌ها صورت می‌گیرد.

جدول (۵). مقایسه طرح پیشنهادی با دو طرح دیگر از لحاظ سربار محاسباتی

Scheme	[52]	[70]	Our Scheme
Encryption	$(5N_e + 1)E + 1E_T$	$(3N_e + 1)E + 1E_T$	$(5N_e + 1)E + 1E_T$
Td Generation	$2E + 1P_e$	$3E$	$2N_wE + N_wP_e$
Key Generation	N_uE	$(2N_u + 1)E$	$2E + 1P_e$
Tran	$N_dE_T + 3N_dP_e$	$N_dE_T + 2N_dP_e$	$2P_e$
Decryption	$1E_T$	$1P_e$	$1E_T$
Search	$2P_e$	$E + P_e$	$0E + 0E_T + 0P_e$

N_u : تعداد ویژگی های کاربر $|G_T|$: اندازه عناصر در گروه جفت نگاشت

N_e : تعداد ویژگی های مرتبط با سیاست رمزنگاری $\log P$: برای نمایش اندازه چکیده یا شاخص

N_w : تعداد کلمات کلیدی جستجو E : عملیات توان گیری در گروه G

$|G|$: اندازه عناصر در گروه بیضوی E_T : عملیات توان گیری در گروه G_T

$|Z_p|$: اندازه عناصر خطی در میدان پایه P_e : عملیات جفت نگاشت

شبیه سازی در رایانه intel® core™ i7-8550U CPU@ 1.80GHz 1.99GHz انجام گرفته، تعداد گره ها از ۱۰ تا ۵۰ گره با افزایش ۵ تایی است. این شبیه سازی توسط نویسنده باهدف بررسی میزان تأخیر در عملکرد الگوریتم در شرایط مختلف و با افزایش تعداد گره ها انجام گرفته است.

در فرایند شبیه سازی، تأخیر در هر مرحله و همچنین تعداد گره ها به صورت متغیر و با استفاده از مقادیر تصادفی شبیه سازی شده اند. طراحی به گونه ای صورت گرفته است که خروجی نهایی بسته به سیستم اجراکننده، نتایج متفاوتی را تولید نماید.

توضیحات الگوریتم PBFT: یک الگوریتم اجماع است که در سیستم های توزیع شده طراحی شده است که قابلیت تحمل خطا داشته و قادر است تا یک سوم از گره های مخرب را مدیریت نماید.

تأخیر تصادفی: در هر مرحله از الگوریتم (درخواست^۱، پیش آماده سازی^۲، آماده سازی^۳، تعهد^۴ و پاسخ^۵) از مقادیر تصادفی استفاده شده است. مقادیر تصادفی با استفاده از random.uniform(min, max) تولید گردیده اند.

گره های تصادفی: در مرحله پیش آماده سازی، گره رهبر^۶ به صورت تصادفی انتخاب شده و زمان انتخاب آن نیز مورد محاسبه قرار گرفته است.

تأخیر با افزایش گره ها: با افزایش تعداد گره ها در مقادیر مختلف (۴، ۸، ۱۶، ۳۲، ۶۴)، مشاهده شده است که زمان مورد نیاز برای اجرای مراحل پیش آماده سازی و تعهد افزایش می یابد. این افزایش تأخیر در نمودار نشان داده می شود.

نمودار تأخیر: میانگین تأخیر برای تعداد گره های مختلف محاسبه و رسم می گردد. در این نمودار رابطه بین تعداد گره ها و تأخیر در اجماع نمایش داده شده است.

ویژگی تصادفی بودن: از آنجاکه در این شبیه سازی از مقادیر تصادفی استفاده شده است، در هر اجرا نتایج متفاوتی مشاهده می گردد.

زمان های تصادفی برای هر مرحله اجماع: تأخیر درخواست مشتری، تأخیر مرحله پیش آماده سازی، تأخیر مرحله آماده سازی، تأخیر مرحله تعهد و تأخیر پاسخ.

محاسبات تصادفی: تعداد گره ها تأثیر مستقیمی بر افزایش تأخیر دارد، اما مقدار دقیق تأخیر در هر اجرا به دلیل استفاده از مقادیر تصادفی متغیر خواهد بود.

با افزایش تعداد ویژگی ها، طول درجه و کلیدهای کاربران افزایش می یابد؛ اما متن رمزی وابسته به حجم متن باقی می ماند. درجه ها برای هر ویژگی حاوی عناصر در گروه G هستند، در حالی که TK در G_T محاسبه می شود. Digest در زنجیره قالب جهت اعتبارسنجی نتیجه جستجو ذخیره می گردد و حجم ثابتی دارد (فرضاً SHA-256، معادل ۲۵۶ بیت).

عملیات راه اندازی شامل تعریف جفت نگاشت دوخطی و تولید پارامترهای عمومی است. TkGen و TdGen در سمت کاربر اجرا می شود و هزینه هایشان با تعداد ویژگی ها مقیاس پذیر است. رمزگشایی جزئی Tran توسط لبه انجام می شود و شامل زوج سازی و توان رسانی می شود. کاربر نهایی فقط ضرب ساده برای بازیابی دانش انجام می دهد (تأیید صحت توسط Digest انجام می شود).

باتوجه به جدول ۵ در مقاله طرح پیشنهادی از لحاظ کاهش دودهای ارتباطی، سرعت بازیابی اطلاعات، بهینه تر می گردد. به دلیل اینکه با درجه فقط تطبیق شاخص روی سرور انجام می شود، جستجو طرح پیشنهادی سبک می گردد. افزایش جزئی هزینه ها به دلیل افزایش امنیت قابل چشم پوشی است.

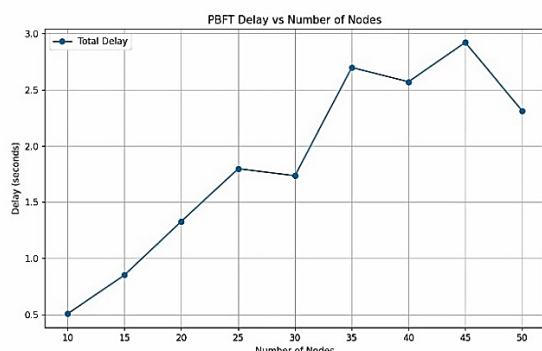
۴. پیاده سازی اجماع PBFT

شبیه سازی الگوریتم اجماع PBFT با استفاده از زبان Python در محیط Visual Studio پیاده سازی شده است.

¹. Request.
². pre-prepare.
³. Prepare.
⁴. Commit.
⁵. Reply.
⁶. Primary.

پردازش پیامها به طور تصادفی محاسبه می شود که منجر به خروجی های متفاوت روی سیستم های مختلف خواهد شد. نمودار تأخیر بر اساس گره ها:

با افزایش تعداد گره ها، تأخیر الگوریتم اجماع با روندی تقریباً خطی یا نمایی افزایش می یابد. بنابراین: افزایش تعداد گره ها، به دلیل افزایش پیام های تبادلی و پردازش بیشتر، باعث افزایش تأخیر می شود. در شبیه سازی این تأخیر به صورت تصادفی مدل سازی شده تا شرایط شبکه و پردازش در سیستم های مختلف بازتاب یابد. علت کاهش زمان اجماع با افزایش تعداد گره ها به دلیل خاصیت مقیاس پذیری خود اجماع PBFT است.



شکل (۶). تأخیر اجماع الگوریتم PBFT با افزایش تدریجی گره ها

۵. نتیجه گیری

باتوجه به رشد روزافزون اینترنت اشیا و گستردگی کاربردهای آن در حوزه های مختلف زندگی روزمره، نیاز به سازوکارهای مؤثر جهت تأمین امنیت، حفظ حریم خصوصی، ناشناس ماندن کاربران و تضمین یکپارچگی اطلاعات احساس می شود. دستگاه های متصل در اینترنت اشیا به صورت مستمر داده هایی را تولید کرده و این داده ها نیازمند جمع آوری و اشتراک گذاری هستند. در کاربردهایی نظیر خانه های هوشمند، مراقبت های بهداشتی و حمل و نقل هوشمند، ضرورت دارد تا داده ها به صورت کنترل شده و هدفمند با افراد خاص به اشتراک گذاشته شوند. به منظور کنترل دسترسی، راهکارهای متعددی تاکنون ارائه شده است. در این پژوهش، طرحی تغییر یافته مبتنی بر مرجع [۲] با ویژگی هایی چون احراز اصالت متقابل بین دامنه ای، حفظ حریم خصوصی، ناشناس ماندن، رمزگشایی جزئی، ابطال دوگانه، جستجوی مبتنی بر کلمه کلیدی برای بازیابی فایل های رمزنگاری شده و فیلترسازی درخواست ها با در نظر گرفتن عدالت در دسترسی پیشنهاد شده است. در این ساختار، دامنه های متعددی در نظر گرفته شده است. کاربران و دستگاه ها، اطلاعات هویتی و ویژگی های خود را به مراجع دامنه محلی مربوط به هر دامنه ارسال می نمایند. سپس، مرجع محلی هر دامنه بر اساس اطلاعات دریافتی، کلیدهای رمزنگاری، توکن های جستجو و دسترسی را ایجاد کرده و یک نسخه از آن ها در اختیار دستگاه ها قرار داده

خروجی منحصر به فرد: هر بار اجرا شبیه سازی، توزیع تصادفی تأخیرها منجر به تولید خروجی متفاوت می شود. میانگین تأخیرها و نمودار بر اساس این تغییرات شکل می گیرند.

تأخیر بر اساس تغییرات گره ها: در اجماع PBFT میزان تأخیر در رسیدن به اجماع تحت تأثیر گره ها و وضعیت شبکه قرار دارد. این تغییرات در سه مرحله اصلی رخ می دهد: پیش آماده سازی، آماده سازی، تعهد. تأثیر تعداد گره ها بر تأخیر به عوامل زیر بستگی دارد:

۱. افزایش تعداد گره ها و تأثیر آن بر پیام ها: پیام های بیشتر: PBFT به ازای هر گره نیازمند تبادل پیام بین تمامی گره ها است. تعداد پیام های تبادلی از مرتبه $O(n^2)$ است، زیرا هر گره باید پیام ها را به همه ارسال کند و از همه پیام دریافت کند. تأخیر ناشی از شبکه: با افزایش تعداد گره ها، ازدحام شبکه^۱ و تأخیر پردازش پیام افزایش می یابد.

فرمول پیام ها:

$$n = total\ message(n - 1) \quad (۵۶)$$

که n تعداد گره ها است.

۲. ارتباط تعداد گره ها با تعداد خطاها^۲ برای تحمل f خطا، تعداد کل گره ها باید، $n = 3f + 1$ باشد؛ بنابراین برای افزایش تعداد گره ها و افزایش تحمل خطا، تأخیر اجماع افزایش می یابد، زیرا زمان بیشتری برای رسیدن به توافق لازم است.

۳. تأثیر تصادفی تأخیر در شبکه: تأخیر برای هر پیام به صورت تصادفی شبیه سازی می شود. این تأخیر شامل: زمان پردازش در گره ها: زمان مورد نیاز برای پردازش درخواست ها در هر گره به طور مستقل در نظر گرفته شده است. زمان انتقال پیام در شبکه: مدت زمان انتقال هر پیام از یک گره به گره دیگر، باتوجه به وضعیت و شرایط شبکه متغیر در نظر گرفته شده است.

۴. رابطه با مراحل PBFT: در هر مرحله، گره ها باید پیام هایی را ارسال و دریافت کنند. با افزایش تعداد گره ها، زمان مورد نیاز برای جمع آوری تأییدیه ها افزایش می یابد:

مرحله پیش آماده سازی: پیام اولیه توسط گره رهبر برای تمامی گره های شبکه ارسال می گردد.

مرحله آماده سازی: پیام رهبر توسط گره ها دریافت و تأیید شده، سپس به سایر گره ها باز ارسال می شود.

مرحله تعهد: گره ها پیام های دریافت شده در مرحله آماده سازی را تحلیل کرده و پیام نهایی تصمیم را منتشر می کنند.

۵. تأخیر تصادفی در شبیه سازی: تأخیرها به صورت تصادفی با تابع (random.uniform) تنظیم شده اند. مقدار تصادفی برای هر گره و هر پیام متفاوت است. در هر اجرا، تعداد گره ها و تأخیر در

^۱. Network congestion.

^۲. Fault tolerance.

شبیه‌سازی‌های مرتبط، مقایسه و شبیه‌سازی طرح پیشنهادی در کارهای آینده ارائه خواهند شد.

قدردانی: از راهنمایی‌های استاد گرامی، جناب آقای دکتر مجید بیات که در پیشبرد این پژوهش یاری‌رسان بودند، صمیمانه تشکر می‌گردد. همچنین از سرکار خانم فاطمه مطیع شیرازی که در مسیر نگارش راهنمایی‌های ارزشمندی ارائه نمودند، سپاسگزاری به عمل می‌آید. قدردانی ویژه نیز از نویسنده همکار، جناب آقای پیمان ویسی به‌واسطه‌ی همراهی در انجام اصلاحات مقاله صورت می‌پذیرد.

۶. مراجع

1. Xiaohan Hao, Wei Ren, Yangyang Fei, Tianqing Zhu, Kim-Kwang Raymond Choo, "A Blockchain-Based Cross-Domain and Autonomous Access Control Scheme for Internet of Things," IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 16, NO. 2, MARCH/APRIL 2023, <https://doi.org/10.1109/TS-C.2022.3179727>
2. Suhair Alshehri, Omairah Bamasq, Daniyal Alghazzawi, Arwa Jamjoom, "Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment," IEEE INTERNET OF THINGS JOURNAL, VOL. 10, NO. 5, 1 MARCH 2023, <https://doi.org/10.1109/IJOT.2022.3217087>
3. Hancheng Gao, Haiping Huang, Lingyan Xue, Fu Xiao, Qi Li, "Blockchain-Enabled Fine-Grained Searchable Encryption With Cloud-Edge Computing for Electronic Health Records Sharing," IEEE INTERNET OF THINGS JOURNAL, VOL. 10, NO. 20, 15 OCTOBER 2023, <https://doi.org/10.1109/IJOT.2023.3279893>
4. Suhui Liu, Liqun Chen, Liqun Chen, Jianchang Lai, "Integrated and Accountable Data Sharing for Smart Grids With Fog and Dual-Blockchain Assistance," IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, <https://doi.org/10.1109/TII.2023.3328831>
5. J. Wang, X. Lin, Y. Wu, and J. Wu, "Blockchain-Enabled Lightweight Fine-Grained Searchable Knowledge Sharing for Intelligent IoT," IEEE Internet of Things Journal, vol. 10, no. 24, pp. 215662-1579, Dec. 2023, <https://doi.org/10.1109/IJOT.2023.3306606>
6. J. Cui, N. Liu, Q. Zhang, D. He, C. Gu, and H. Zhong, "Efficient and Anonymous Cross-Domain Authentication for IIoT Based on Blockchain," IEEE Transactions on Network Science and Engineering, vol. 10, no. 2, pp. 899-910, Mar. 2023, <https://doi.org/10.1109/TNSE.2022.3224453>
7. J. Yu, S. Liu, M. Xu, H. Guo, F. Zhong, and W. Cheng, "An Efficient Revocable and Searchable MA-ABE Scheme With Blockchain Assistance for C-IoT," IEEE Internet of Things Journal, vol. 10, no. 3, pp. 2754-2766, Feb. 2023, <https://doi.org/>

می‌شود. این اطلاعات در زنجیره قالب اول ذخیره می‌گردند و همچنین، در انباشتگر پویا تجمیع می‌شوند که با قرارداد هوشمند فراخوانی می‌شود [۶]. در احراز اصالت بعدی، برای افزایش سرعت از اطلاعات موجود در انباشتگر استفاده شده است. در فرایند ثبت‌نام اولیه، از الگوریتم اجماع و زنجیره استفاده می‌شود، درحالی‌که در مراحل بعدی برای کاهش دوره‌های ارتباطی و کاهش تأخیر، تنها از انباشتگر بهره‌برداری می‌گردد. در زمان ارسال درخواست از یک دامنه به دامنه دیگر، ابتدا درخواست به گره دروازه ارسال شده و با توجه به معیارهایی چون احراز هویت، تازگی درخواست و مهر زمانی، عملیات فیلتر انجام می‌پذیرد. سپس درخواست به گره‌های لبه ارسال می‌شود. این گره‌ها با بهره‌گیری از مکانیزم‌های بهینه‌سازی و اجماع، گره‌های مناسب برای تفویض دسترسی را انتخاب کرده و از طریق یک کانال امن با لبه دامنه هدف، اطلاعات مربوط به درخواست، ویژگی‌ها، قراردادهای دسترسی و جستجو را تبادل می‌نمایند. در ادامه، عملیات رمزگشایی جزئی توسط گره لبه انجام گرفته و به کاربر درخواست‌کننده ارسال می‌شود [۵]. تکمیل فرایند رمزگشایی و بازیابی فایل توسط خود کاربر صورت می‌گیرد. مالک داده‌ها، اطلاعات را به همراه ساختار دسترسی و سیاست جستجو با بهره‌گیری از رمزنگاری مبتنی بر ویژگی، در فضای ابری بارگذاری می‌کند. همچنین، مرجعی جهانی در فضای ابری تعریف شده که با نگهداری نسخه‌ای از اطلاعات مراجع محلی، اشتراک‌گذاری بین دامنه‌ای را تسهیل می‌نماید. در این ساختار، زنجیره قالب دومی در نظر گرفته شده که چکیده‌ای از اطلاعات را در خود جای داده و امکان جستجو در فضای ابری را بر مبنای قراردادهای جستجو و دسترسی فراهم می‌سازد [۴]. به‌منظور کنترل دسترسی پویا، از ابطال دوگانه بهره گرفته شده است؛ به‌گونه‌ای که کاربران مخرب بر اساس رفتار شناسایی و حذف می‌شوند و ویژگی‌ها نیز با رسیدن به زمان انقضا اعتبار خود را از دست می‌دهند. برای هر دامنه یک آستانه تعریف شده است. بدین ترتیب، طرح پیشنهادی از جنبه‌های زمان احراز اصالت، عدالت در دسترسی، جستجوی مبتنی بر کلمه کلیدی و بررسی هم‌زمان یکپارچگی و احراز هویت، بهبود یافته است. همچنین، طرح مذکور در برابر حملاتی نظیر انکار سرویس، جعل هویت، تکرار مقاوم است. در ادامه، یک شبیه‌سازی ساده از الگوریتم اجماع مورد استفاده PBFT پیاده‌سازی شده است تا تأثیر افزایش تعداد گره‌ها بر تأخیر اجماع بررسی گردد. این افزایش تأخیر ناشی از تبادل پیام میان گره‌ها بوده و برای کاهش آن از انباشتگر پویا استفاده شده است. به‌نحوی که از زنجیره و اجماع تنها در مرحله اولیه ثبت‌نام بهره گرفته می‌شود و در مراحل بعدی، احراز اصالت از طریق اطلاعات موجود در انباشتگر انجام می‌پذیرد. این رویکرد موجب کاهش دوره‌های ارتباطی، کاهش تأخیر و افزایش سرعت شده است. سایر

- DigitalObjectIdentifier, <https://doi.org/10.1109/ACCESS.2022.3230944>
18. Peng Wang, Ning Xu, Haibin Zhang, Wen Sun, Abderrahim Benslimane, "Dynamic Access Control and Trust Management for Blockchain empowered IoT," : <https://doi.org/10.1109/JIoT.2021.3125091>, IEEE Internet of Things Journal
19. Xin Wei, Yong Yan, Shaoyong Guo, Xuesong Qiu, and Feng Qi, "Secure Data Sharing: Blockchain enabled Data Access Control Framework for IoT," JOURNAL OF LATEX CLASS FILES, VOL. 14, NO. 8, AUGUST 2015, <https://doi.org/10.1109/JIoT.2021.3111012>
20. Kwame Opuni-Boachie Obour Agyekum, Qi Xia, Emmanuel Boateng Sifah, Christian Nii Aflah Cobblah, Hu Xia, Jianbin Gao, "A Proxy Re-Encryption Approach to Secure Data Sharing in the Internet of Things Based on Blockchain," IEEE SYSTEMS JOURNAL, VOL. 16, NO. 1, MARCH 2022, <https://doi.org/10.1109/JSYST.2021.3076759>
21. Saiyu Qi, Xu Yang, Jiahe Yu, and Yong Qi, "Blockchain-Aware Rollbackable Data Access Control for IoT-Enabled Digital Twin," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 41, NO. 11, NOVEMBER 2023, <https://doi.org/10.1109/JSAC.2023.3310061>
22. Zia Ullah, Basit Raza, Habib Shah, Shahzad Khan, D Abdul Waheed, "Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment," Digital Object Identifier , <https://doi.org/10.1109/ACCESS.2022.3164081>
23. Zeeshan Zulkifl, Fawad Khan, Shahzaib Tahir, ..., "FBASHI: Fuzzy and Blockchain-Based Adaptive Security for Healthcare IoTs," Digital Object Identifier , <https://doi.org/10.1109/ACCESS.2022.3149046>
24. Omaji Samuel, Akogwu Blessing Omojo, Syed Muhammad Mohsin, Prayag Tiwari, Deepak Gupta, Shahab S. Band, "An Anonymous IoT-Based E-Health Monitoring System Using Blockchain Technology," IEEE SYSTEMS JOURNAL, VOL. 17, NO. 2, JUNE 2023, <https://doi.org/10.1109/JSYST.2022.3170406>
25. Lihua Zhang, Boping Li , "An Internet of Things Access Control Scheme Based on Permissioned Blockchain and Edge Computing," 2023 by the authors. Licensee MDPI, Basel, Switzerland. Appl.Sci.2023,13,4167, <https://doi.org/10.3390/app13074167>
26. Oscar Novo, "Blockchain Meets IoT: an Architecture for Scalable Access Management in IoT," JOURNAL OF INTERNET OF THINGS CLASS FILES, VOL. 14, NO. 8, MARCH 2018, <https://doi.org/10.1109/JIoT.2018.2812239>
27. J. Lu, W. Li, J. Sun, R. Xiao, and B. Liao, "Secure and Real-Time Traceable Data Sharing in Cloud-Assisted IoT," IEEE Internet of Things Journal, vol. 11, no. 4, pp. 10.1109/JIoT.2022.3213829.
8. S. Wang, J. Ye, and Y. Zhang, "A keyword searchable attribute-based encryption scheme with attribute update for cloud storage," PloS one, vol. 13, no. 5, 2018, Art. no. e0197318. <https://doi.org/10.1371/journal.pone.0197318>
9. Jegadeesan Subramani, Azees Maria, "Blockchain-Based Physically Secure and Privacy-Aware Anonymous Authentication Scheme for Fog-Based VANETs," Digital ObjectIdentifier, <https://doi.org/10.1109/ACCESS.2022.3230448>.
10. Somchart Fugkeaw, Leon Wirz, Lyhour Hak, "Secure and Lightweight Blockchain-Enabled Access Control for Fog-Assisted IoT Cloud Based Electronic Medical Records Sharing," DigitalObjectIdentifier, <https://doi.org/10.1109/ACCESS.2023.3288332>
11. Arezou Zamanyzadeh Abyaneh, Nizar Zorba, Bechir Hamdaoui, "Empowering Next-Generation IoT WLANs Through Blockchain and 802.11ax Technologies," IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 24, NO. 7, JULY 2023, <https://doi.org/10.1109/TITS.2022.3153484>
12. Aditya Pathak, Irfan Al-Anbagi, Howard J. Hamilton, "TABI: Trust-Based ABAC Mechanism for Edge-IoT Using Blockchain Technology," Digital Object Identifier <https://doi.org/10.1109/ACCESS.2023.3265349>
13. Sivaselvan N, Vivekananda Bhat K, Muttukrishnan Rajarajan, Ashok Kumar Das, "A New Scalable and Secure Access Control Scheme using Blockchain Technology for IoT," publication in IEEE Transactions on Network and Service Management. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: <https://doi.org/10.1109/TNSM.2023.3246120>.
14. Hongzhi Li, Dezhi Han, Chin-Chen Chang, "DAC4SH: A Novel Data Access Control Scheme for Smart Home Using Smart Contracts," IEEE SENSORS JOURNAL, VOL. 23, NO.6, 15 MARCH 2023, <https://doi.org/10.1109/JSEN.2023.3241093>
15. Dezhi Han, Yujie Zhu, Dun Li, Wei Liang, Alireza Souri, Kuan-Ching Li, "A Blockchain-Based Auditable Access Control System for Private Data in Service-Centric IoT Environments," IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 18, NO. 5, MAY 2022, <https://doi.org/10.1109/TII.2021.3114621>
16. Shuang Sun , Rong Du, Shudong Chen, Weiwei Li, "Blockchain-Based IoT Access Control System: Towards Security, Lightweight, and Cross-Domain," Digital Object Identifier <https://doi.org/10.1109/ACCESS.2021.3059863>
17. Fathe Jeribi, Rashid Amin, Mohammed Alhameed, D Ali Tahir, "An Efficient Trust Management Technique Using ID3 Algorithm With Blockchain in Smart Buildings IoT,"

38. D. Wang, B. Li, B. Song, Y. Liu, K. Muhammad, and X. Zhou, "Dual-Driven Resource Management for Sustainable Computing in the Blockchain-Supported Digital Twin IoT," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 65496560, Apr. 2023, <https://doi.org/10.1109/JIOT.2022.3162714>.
39. K. Zhang, M. Deng, B. Gong, Y. Miao, and J. Ning, "Privacy-Preserving Traceable Encrypted Traffic Inspection in Blockchain-Based Industrial IoT," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 3484–3496, Jan. 2024, <https://doi.org/10.1109/JIOT.2023.3297601>.
40. J. Wang, X. Lin, Y. Wu, and J. Wu, "Blockchain-Enabled Lightweight Fine-Grained Searchable Knowledge Sharing for Intelligent IoT," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21566–21579, Dec. 2023, <https://doi.org/10.1109/JIOT.2023.3306606>.
41. L. Zhang, X. Li, Q. Wu, and F. Rezaeiabgha, "Blockchain-Aided Anonymous Traceable and Revocable Access Control Scheme With Dynamic Policy Updating for the Cloud IoT," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 526–542, Jan. 2024, <https://doi.org/10.1109/JIOT.2023.3287190>.
42. Feiffi Guo, Guohua Shen, "DABAC: Smart Contract-Based Spatio-Temporal Domain Access Control for the Internet of Things," *Digital Object Identifier*, <https://doi.org/10.1109/ACCESS.2023.3257027>.
43. Zhuo Ma, Jiawei Zhang, "Efficient, Traceable and Privacy-Aware Data Access Control in Distributed Cloud-Based IoD Systems," *Digital Object Identifier*, <https://doi.org/10.1109/ACCESS.2023.3272484>.
44. Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi, "Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management," *IEEE TRANSACTIONS ON COMPUTATIONAL SOCIAL SYSTEMS*, VOL. 10, NO. 4, AUGUST 2023, <https://doi.org/10.1109/TCSS.2022.3186945>.
45. Carles Anglés-Tafalla, Alexandre Viejo, Jordi Castellà-Roca, Macià Mut-Puigserver, M. Magdalena Payeras-Capellà, "Security and Privacy in a Blockchain-Powered Access Control System for Low Emission Zones," *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS*, VOL. 24, NO. 1, JANUARY 2023, <https://doi.org/10.1109/TITS.2022.3211659>.
46. Yuming Feng, Weizhe Zhang, Senior Member, IEEE, Xiapu Luo, Bin Zhang, "A Consortium Blockchain-based Access Control Framework with Dynamic Orderer Node Selection for 5G-enabled Industrial IoT," *IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS*, <https://doi.org/10.1109/II.2021.3078183>.
47. Tanzeel Zaidi, Muhammad Usman, Muhammad Umar Aftab, "Fabrication of Flexible Role-Based
- 65216536, Feb. 2024, <https://doi.org/10.1109/JIOT.2023.3314764>.
28. J. Liu, Y. Fan, R. Sun, L. Liu, C. Wu, and S. Mumtaz, "Blockchain-Aided Privacy-Preserving Medical Data Sharing Scheme for E-Healthcare System," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 21377–21388, Dec. 2023, <https://doi.org/10.1109/JIOT.2023.3287636>.
29. K. Zhang, Y. Zhang, Y. Li, X. Liu, and L. Lu, "A Blockchain-Based Anonymous Attribute-Based Searchable Encryption Scheme for Data Sharing," *IEEE Internet of Things Journal*, vol. 11, no. 1, pp. 1685–1697, Jan. 2024, <https://doi.org/10.1109/JIOT.2023.3290975>.
30. Y. Liu et al., "A Blockchain-Based Cross-Domain Authentication Management System for IoT Devices," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 1, pp. 115127, Jan. 2024, <https://doi.org/10.1109/TNSE.2023.3292624>.
31. J. Y. Lee, J. Oh, D. K. Kwon, M. Kim, K. Kim, and Y. Park, "Blockchain-Enabled Key Aggregate Searchable Encryption Scheme for Personal Health Record Sharing With Multi-Delegation," *IEEE Internet of Things Journal*, 2024, <https://doi.org/10.1109/JIOT.2024.3357802>.
32. K. Zhang, M. Deng, B. Gong, Y. Miao, and J. Ning, "Privacy-Preserving Traceable Encrypted Traffic Inspection in Blockchain-Based Industrial IoT," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 3484–3496, Jan. 2024, <https://doi.org/10.1109/JIOT.2023.3297601>.
33. G. Chen et al., "A Lightweight Authentication-Driven Trusted Management Framework for IoT Collaboration," *IEEE Transactions on Services Computing*, 2024, <https://doi.org/10.1109/TSC.2023.3349305>.
34. K. Fan et al., "SC-Chain: An Efficient Blockchain Framework for Smart City," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7863–7877, Mar. 2024, <https://doi.org/10.1109/JIOT.2023.3317451>.
35. J. Yu, B. Yan, H. Qi, S. Wang, and W. Cheng, "An Efficient and Secure Data Sharing Scheme for Edge-Enabled IoT," *IEEE Transactions on Computers*, vol. 73, no. 1, pp. 178–191, Jan. 2024, <https://doi.org/10.1109/TC.2023.3325668>.
36. R. Guo, G. Yang, H. Shi, Y. Zhang, and D. Zheng, "O3-R-CP-ABE: An Efficient and Revocable Attribute-Based Encryption Scheme in the Cloud-Assisted IoMT System," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 89498963, Jun. 2021, <https://doi.org/10.1109/JIOT.2021.3055541>.
37. Y. Zhang, X. Wang, X. He, N. Zhang, Z. Zheng, and K. Xu, "Galaxy: A Scalable BFT and Privacy-Preserving Pub/Sub IoT Data Sharing Framework Based on Blockchain," *IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 52225236, Feb. 2024, <https://doi.org/10.1109/JIOT.2023.3307073>.

50. Zijian Bao, Debiao He, Huaqun Wang, Min Luo, Cong Peng," A Group Signature Scheme with Selective Linkability and Traceability for Blockchain-Based Data Sharing Systems in E-health Services," publication in IEEE Internet of Things Journal. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: <https://doi.org/10.1109/JIOT.2023.3284968>.
51. Jiawei Zhang , Yanbo Yang , Ximeng Liu, Jianfeng Ma," An Efficient Blockchain-Based Hierarchical Data Sharing for Healthcare Internet of Things," IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 18, NO. 10, OCTOBER 2022, <https://doi.org/10.1109/TII.2022.3145851>
- Access Control Based on Blockchain for Internet of Things Use Cases," Digital Object Identifier <https://doi.org/10.1109/ACCESS.2023.3318487>
48. Fei Tong, Xing Chen, Cheng Huang, Yujian Zhang, Xuemin Shen," Blockchain-Assisted Secure Intra/Inter-Domain Authorization and Authentication for Internet of Things," IEEE INTERNET OF THINGS JOURNAL, VOL. 10, NO. 9, 1 MAY 2023, <https://doi.org/10.1109/JIOT.2022.3229676>
49. Marah R. Bataineh, Wail Mardini, Yaser M. Khamayseh, D Muneer Masadeh Bani Yassein," Novel and Secure Blockchain Framework for Health Applications in IoT," Digital Object Identifier <https://doi.org/10.1109/ACCESS.2022.3147795>